Assessment of Cloud Computing Readiness of Financial Institutions in South Africa

A mini dissertation presented to the

Department of Information Systems

University of Cape Town

By:

Akande Akinlolu Olumide

Student Number: AKNAKI006

In partial fulfilment of the requirements for the

Master of Commerce in Information Systems

(INF5005W)

Supervisor: Professor Jean-Paul Van Belle

February 2014

Plagiarism Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in this Dissertation "**Assessment of Cloud Computing Readiness of Financial Institutions in South Africa**" from the work(s) of other people has been attributed, and has been cited and referenced.

3. This Dissertation "**Assessment of Cloud Computing Readiness of Financial Institutions in South Africa**" is my own work.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

5. I acknowledge that copying someone else's dissertation or part of it is wrong, and declare that this is my own work.

Signed by candidate

Signature: Signature Removed **Date: 01/02/2014**

Full Name of Student: Akande Akinlolu Olumide

Acknowledgements

I would like to thank God for the grace to complete this work. I would also like to thank my supervisor, Professor Jean-Paul Van Belle whose guidance and advice has greatly contributed to the success of this dissertation. I appreciate his invaluable and professional contribution to this research.

Secondly, I would like to thank my course convenor, Professor Michael Kyobe for his encouragement and advice as it kept me going throughout my research.

Furthermore, I would like to thank the National Research Foundation (NRF) for their financial support towards the success of this research. The assistance I received from NRF is much appreciated has it helped in ensuring the success of this research.

I would also like to thank my parents Chief Oladapo Akande and Mrs Florence Ajoke Akande for their support and encouragement which gave me strength to successfully complete this work.

Finally, I would like to thank my darling, Nozuko for her unending support for my studies. Thank you all for your support for without all the assistance and support I received from you all, it would have been difficult to complete this research.

Publications based on this research

Akande , A. O., & Van Belle, J.-P. (2013). Management Issues with Cloud Computing. *Proceedings of the IEEE International Conference on Cloud Computing* (pp. 1 - 6). Wuhan, China: IEEE eXplore.

Akande, A. O., & Van Belle, J.-P. (2013). Towards the Development of a Framework to Increase the Cloud Computing Readiness of Financial Institutions in South Africa. *Proceedings of the IEEE International Conference on E-Leadership: Technology Innovation and Leadership in an Electronic Age* (pp. 111 -116). Pretoria, South Africa: IEEE eXplore.

Akande, A. O., April, N. A., & Van Belle, J.-P. (2013). ICT Adoption in South Africa: Opportunities, Challenges and Implications for national development. *Proceedings of the IEEE International Conference on Electronics Technology and Industrial Development* (pp. 28 - 33). Bali, Indonesia: Association for Computing Machinery.

Abbreviations and Acronyms

ADSL - Asymmetric digital subscriber line

APIs - Application Programming Interfaces

AWS - Amazon Web Services

B1 - Bank 1

B2 - Bank 2

B3 - Bank 3

B4 - Bank 4

BCCR - Becoming Cloud Computing Ready

BCDR - Business Continuity and Disaster Recovery

BPOS - Business Productivity Online Standard Suite

C1 - Consultant 1

C2 - Consultant 2

C3 - Consultant 3

C4 - Consultant 4

CC - Cloud Computing

CF1 - Consulting Firm 1

CF2 - Consulting Firm 2

CF3 - Consulting Firm 3

CF4 - Consulting Firm 4

CPU - Central Processing Unit

CRM - Customer Relationship Management

EC2 - Amazon Elastic Compute Cloud

ECA - Electronics Communications Act

I1 - Insurance 1

I2 - Insurance 2

I3 - Insurance 3

I4 - Insurance 4

IaaS - Infrastructure as a Service

IBM - International Business Machines

ICCC - International Conference on cloud Computing

IPS - Intrusion Protection Systems

IS - Information Systems

IT - Information Technology

JSE - Johannesburg Stock Exchange

MTTR - Mean Time To Recovery

NIST - National Institute of Standards and Technology

PaaS - Platform as a Service

PB1 - Participant Bank 1

PB2 - Participant Bank 2

PB3 - Participant Bank 3

PB4 - Participant Bank 4

PI1 - Participant Insurance 1

PI2 - Participant Insurance 2

PI3 - Participant Insurance 3

PI4 - Participant Insurance 4

PIA - Promotion of Access to Information Act

POPI - Protection of Personal Information

QDA - Qualitative Data Analysis

QoS - Quality of Service

ROI - Return On Investments

SA - South Africa

SaaS - Software as a Service

SLAs - Service Level Agreements

TOE - Technology, Organisation and Environment

UCT - University of Cape Town

UK - United Kingdom

USA - United States of America

VMs - Virtual Machines

Abstract

Cloud Computing (CC) is becoming popular among organisations from different industries in South Africa (SA) because of its promises such as cost reduction, on demand self-service, broad access network, resource pooling , rapid elasticity , measured service, little or no set up capital and faster time to market. As a result, many organisations are already in the early stages of their CC implementation while others are planning to adopt CC.

Although CC promises many benefits, it is equally important to note that there are some barriers to its adoption which needs to be considered before adoption in order to ensure implementation success. Proper understanding of these barriers and coming up with ways to mitigate them will improve the CC readiness level of organisations.

Among the various industry sectors, the financial industry in SA has been one of the early adopters of CC but they have not fully implemented it because of barriers such as security and privacy (Vignos, Kim, & Metzer, 2013), governance issues, inadequate cloud service level agreements (SLAs), vendor lock in, poor vendor transparency, inability to assess risks, confidentiality, integrity and availability. Because CC is relatively new and is still in its early stages, not much work has been done to inform organisations about the barriers and enablers of CC. Available guidelines to help organisations improve their CC readiness level are also inadequate. This is risky for financial institutions that deal with sensitive customer information as the safety of that information is not guaranteed if a desired readiness level is not attained before implementation.

In order to assist financial institutions with this hurdle, this research identified and discuss the barriers and enablers of CC in order to be able to come up with solutions to the barriers. This research also developed a framework that will serve as a tool by which financial institutions can determine and improve their CC readiness.

The framework is called “Becoming Cloud Computing Ready” (BCCR) and it will assist financial institutions to determine which stage they are with their CC readiness. It will also provide guidelines that will assist financial institutions to improve their level of readiness in order to ensure successful CC adoption.

Furthermore, this research discussed the various service and deployment models of CC and present important factors necessary for successful CC adoption. If financial institutions are able to follow the guidelines given by the proposed BCCR framework, their CC readiness level will be improved and they will benefit from a successful CC implementation.

This research collected data from interviews and literature. The data was analysed using thematic analysis. The outcomes of the interviews were in line with literature and the validated the works of other resarchers in this field. The researcher ensured the validity of the data and framework by sending the results to the participants. The participants' responses showed that the results met the expectations of the participants and the framework would be able to guide them towards their CC implementation. The researcher also validated the data and framework by presenting them at different academic conferences in which other researchers were able to provide useful comments.

Keywords: Cloud Computing, cloud, adoption, implementation, financial institutions, organisations, readiness, banks, insurance companies, strategy, change management, consultant, cloud provider, service provider, BCCR

Table of Contents

List of figures

List of tables

1. Introduction and Background

This chapter presents the introduction of this study by giving a general overview of CC and presenting the background of this study. The problem statement, motivation, gaps in literature, research objectives, research question, relevance of this research to the financial institution, SA and the research community are also discussed in this chapter. The assumptions made by the researcher and the expected limitations are also discussed in this chapter. The final section of this chapter gives a general overview of this dissertation.

1.1 Introduction

CC is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Canedo, de Sousa Junior, & de Oliveira, 2012). CC has become prevalent among organisations looking for a cheaper way to access needed infrastructure, service, and/or applications (Paquette, Jaeger, & Wilson, 2010) and has changed organisations perception of software, infrastructures and development platforms (Zissis & Lekkas, 2012).

CC is fast becoming a necessity for organisations to remain competitive and do their business faster with less resource than they would have used without CC (Goldstuck, 2011). CC helps remove the cost of buying, installing, maintaining and upgrading hardware. Other benefits of CC includes scalability, ubiquity, flexibility, and its deployment is quick and easy (Goldstuck, 2011).

This dissertation details a study on the assessment of CC readiness of financial institutions in SA. Readiness is the ability of an organisation to successfully adopt, use, and benefit from a technology (Fathian, Akhavan, & Hoorali, 2008). CC readiness can therefore be defined as the ability of an organisation to successfully adopt, use, and benefit from CC. The lack of readiness for a technology before adoption has led to implementation failure of many technology initiatives (Snyder, 2001) and this shows that it is important for organisations to assess their readiness before adopting CC.

The aim of this study is to assess the CC readiness level of financial institutions in SA, identify the barriers and enablers of CC and to propose and develop an integrated framework which will serve as an instrument by which financial institutions can measure their CC readiness.

1.2 Background

CC is no doubt a revolutionary technology that is changing the way organisations carry out their daily activities. There are different cloud delivery models, all of which are based on a pay per use model (Misra & Mondal, 2011; Yeo, Venugopal, Chu, & Buyya, 2010).

Gong, Liu, Zhang, Chen, & Gong, (2010) referred to clouds as a large pool of virtualized resources which are easy to use and access and they further identified ten characteristics of CC which includes user friendliness, virtualization, Internet centric, variety of resources, automatic adaptation, resource optimization, Service-Level Agreements (SLAs) and infrastructure SLAs. Although CC offers a lot of benefits, it is important to note that it also has some limitations so that organisations can be aware of these limitations and take necessary precautions to prevent problems which may arise as a result of these limitations.

Tsai, Sun, & Balasooriya, (2010) identified some of the limitations of CC which are: users are often tied with one cloud provider because of the lack of standardised application programming interfaces (APIs), computing components are tightly coupled, lack of SLA supports, lack of multi-tenancy supports, and lack of flexibility for user interface.

With the benefits of CC usually outweighing its disadvantages and limitations, more and more organisations are moving into the cloud while others are seriously considering moving as well. During the IP EXPO Corporate Cloud Survey 2011, one hundred large Johannesburg Stock Exchange (JSE) listed corporations in SA were interviewed and forty six percent (46%) are already using CC while six percent (6%) planned to introduce it in 2012 and another four percent (4%) in 2013 (Goldstuck, 2011). Thirteen percent (13%) of the total sample said CC was not important for their business as they didn't see any benefit while others don't want to move into the cloud because of poor infrastructure or security concerns but most companies that are still reluctant to adopt CC are inhibited mainly by a lack of understanding (Goldstuck, 2011).

Financial institutions keep large volumes of customer information. This usually requires them to purchase resources such as computers, servers, applications etc. and employ the services of employees who will service and maintain the resources. CC will help to reduce this cost as it will eliminate the need for purchase and maintenance of these resources (Sharma, 2012).

Expansion of financial institutions into the rural areas with inadequate infrastructure also requires the need of CC to provide those branches in rural areas with the standard infrastructures that will enable them do their work properly.

The integrated model that was developed in this research helped to identify all the necessary components of CC and suggest important steps to take before adopting and implementing CC.

1.3 Problem statement, motivation and gaps in literature

1.3.1 Problem statement

Many organisations adopt technologies without considering their level of readiness for that technology and this leads to weak implementation and sometimes failure. In the case of CC, this is mostly as a result of lack of awareness and lack of a regulatory framework for CC implementation (Kshetri, 2010). In order to avoid the problem of weak implementation and failure, there is an urgent need for researchers to come up with tools which will guide organisations and improve their CC readiness level before they finally adopt CC to ensure successful CC implementation.

1.3.2 Motivation and gaps in literature

Although CC has been widely embraced by different organisations, research in CC is still in their early stages (Wang, Rashid, & Chuang, 2011). Most of the current research in the field of CC is focused on the adoption, diffusion, implementation and impact of CC on IT development practices (Wang, Rashid, & Chuang, 2011). Research on CC readiness is minimal. This needs urgent attention because readiness is a phase before adoption and it is an essential factor in determining the success of adoption because lack of readiness has been found to account for majority of the failures in technology adoption. Table 1 shows the status of current CC research from organisation as well as technical stand point. Table 1 reveals that a lot of research has been conducted on CC adoption, privacy, security and trust issues in CC, and service oriented design and development. Table 1 also shows that very little research has been conducted on analytics (Business Intelligence) using cloud and reliability of cloud while few researches has focused on social issues in CC and cloud workflow management. It is however evident from Table 1 that research focus has not been on organisational readiness of CC as most of the research has focused on the implementation and post implementation phases leaving the pre-implementation phase less researched.

Topic	Status (till 2011)	Status (2012 – 2013)	Related Reference
Analytics (Business Intelligence) using Cloud	Very few	Few	[Mircea et al. 2011]
Reliability of Cloud	Very few	Few	[Vogels 2008; Dabrowski 2009]
Social Issues in Cloud computing	Few	Few	[Kim et al. 2008; Provos et al. 2009]
Cloud Workflow Management	Few	Few	[Liu et al. 2010; Wu et al. 2010]
Privacy, Security and Trust issues in Cloud computing	Abundance	Abundance	[Anthens 2010; Carlin & Curran 2011; Grobauer et al. 2011; Kaufman 2009 ;Zissis & Lekkas, 2012]
Service Oriented Design and Development	Abundance	Abundance	[Chen & Meixell 2003; Curley 2006; Elfatatry & Layzell 2004; Huhns & Singh 2005; Hirschheim et al. 2010; Perepletchikov 2008]
Cloud computing Adoption	Abundance	Abundance	[Grossman et al. 2009; Low et al. 2011; Misra & Mondal 2010; Tuncay 2010]
Resource Allocation	Very few	Few	[Valentini et al 2011; Ergu et al, 2013]
Mobile cloud	Few	Few	[Rao, Sasidhar & Kumar 2012; Dinh, Lee, Niyato and Wang 2013]

Table 1: Cloud computing research from Wang, Rashid, & Chuang, (2011, pg. 240) updated 2012-2013

Most of the previous research in this area was conducted in United States (US) and in some cases United Kingdom (UK) and Australia and their research on readiness is also minimal. This research would adopt some of the ideas from the previous studies but will focus on readiness which makes it different and unique. With regards to academic literature on CC readiness, not much has been done in SA and only industry researchers have looked into CC readiness. The research from industry cannot be compared with academic research because industry research may contain elements of advertisement and promotions which are often not purely about the technology in question. Another

reason why industry research cannot be compared with academic research is that in most cases, they only focus on the benefits of the technology and not on its limitations.

1.4 Objectives and research question

1.4.1 Objectives

The main objective of this research is to determine the level of CC readiness of financial institutions in SA. The barriers and enablers of CC readiness of financial institutions in SA will also be identified by conducting interviews with relevant stakeholders. This research also aims to propose and develop an integrated framework which will serve as an instrument by which the CC readiness of financial institutions in SA can be determined and improved.

1.4.2 Research questions

1. What is the level of CC readiness of SA financial institutions?

2. What are the perceived barriers and enablers of CC readiness of SA financial institutions?

3. Can a framework that will assist financial institutions in determining and improving their CC readiness level be developed?

1.5 Relevance of the study

This study will help increase the chances of success for financial institutions with CC implementation. It will benefit financial institutions, the research community and SA.

1.5.1 Relevance to financial institutions

Financial Institutions will benefit from the research because the integrated framework which will be produced by the research will assist financial institutions in reducing the risks involved in the adoption of CC by creating more awareness of CC and informing organisations on what to do to have the necessary capability of implementing CC successfully. These will help SA's financial institutions increase their level of readiness and increase implementation success thereby reducing the level of innovation risk, and leading to a more successful IT/S innovation outcome (Snyder, 2001). The output of this research will also enable organisations to increase their agility, mobility, and ensure faster time to market by providing financial institutions with a framework which can increase their level of CC readiness and lead to successful implementation of CC (Goyal, 2010).

1.5.2 Relevance to South Africa

In March 2012, a new CC study released by Microsoft, and conducted by analyst firm IDC forecasts that CC will lead to creation of around 14 million jobs across the globe by 2015 with nearly 145 000 of those in SA (iTWeb, 2012). Around 62 000 jobs were estimated to be created in SA in 2012 alone through CC initiatives, and this was expected to increase to 82 000 in 2013 (iTWeb, 2012). This research hopes to contribute to the creation of jobs through the creation of awareness of CC in financial institutions which will lead to a successful implementation of CC and subsequently, the creation of jobs. The benefit of job creation could also be realised by financial institutions in other countries that are in the same level of readiness with their SA counterparts if they adopt and use the proposed integrated model that will be developed from this research. CC will also lead to increased competitiveness in SA (Goyal, 2010). The proposed framework will also guide government departments in their CC adoption and lead to improved service delivery and a wider citizenship participation.

1.5.3 Relevance to research community and the field of information systems

The research community will benefit from this research because it will contribute to the existing body of knowledge, especially in the area of CC through the production of an integrated framework which will be a tool for researchers to further investigate CC readiness level of organisations. This study will contribute to CC body of knowledge in SA because only industry researchers have been conducting research on CC readiness of organisations and academic literature is presently limited on this issue.

1.6 Assumptions and limitations

It was assumed that a significant number of SA financial institutions were already using one form of CC or the other and possessed the required knowledge and expertise to answer the questions during the interviews. Getting hold of the participants was a limitation. In order to encourage the participants, the researcher promised to provide them with feedback on the study results. Another limitation is that local literature in this area is minimal which was why this research applied the results of researches from other countries like US, UK and Australia (macro level) to the SA Context (micro level). The time available to conduct the research is another limiting factor because this study is part of the requirement for the completion of master's degree in Information Systems and the time is restricted by duration of the course. Because of this limitation, this study will select only a small sample size that can be interviewed during the available time frame.

1.7 Overview of the dissertation

The remaining sections of the dissertation has been organised as follows. Chapter 2 will give details of the literature review by discussing various issues relating to this research from the literature. The different types of CC, benefits of CC and issues with CC will be discussed in sections 2, 3 and 4 respectively. Section 5 will discuss financial institutions in relation to CC. Section 6 will discuss CC in SA while section 7 will discuss readiness in the context of this research. Section 8 will discuss some important considerations for organisations before adoption of CC. Finally, change management will be discussed in section 9.

Chapter 3 will discuss the research design and methodology of this research by discussing the methodology, underlying philosophy, research approach, research strategy, data collection, validity, limitations and research timeframe. Ethics and confidentiality issues of this research will also be discussed in chapter 3. Data analysis will be discussed in chapter 4. Chapter 5 will present the BCCR framework which is proposed to be a framework that can serve as a tool that will assist financial institutions to determine whether they are ready for CC adoption and also to improve their level of CC readiness. The BCCR framework was developed based on the TOE framework, the change management process and the data obtained from the interviews. Chapter 6 will discuss the conclusions and recommendations. The research limitations, research contributions and areas of future research will also be discussed in chapter 6. Chapter 7 will provide a complete reference list to all the materials used in this research while chapter 8 will provide the appendices.

1.8 Summary of chapter

Many organisations are turning to CC because of its numerous promises such as cost reduction, scalability, ubiquity, flexibility, faster time to market and ease of use. In order to reap the promises of CC, organisations need to assess their level of readiness and to improve on their current readiness level to ensure that their CC adoption is successful and the benefits of CC are realised. Although CC has a lot of benefits, there are some limitations which include security and privacy issues, lack of SLA supports and possibility of vendor lock in etc.

Organisations, especially financial institutions that handle sensitive customer information need a framework that will assist them to assess and improve their cloud readiness level in order to overcome the limitations of CC. In order to achieve this, the research aim to determine the level of CC readiness of SA financial institutions, identify the barriers and enablers of CC and develop a

framework that will serve as a tool by which financial institutions in SA can assess and improve their CC readiness level.

2. Review of literature

This chapter presents a critical review of literature that addresses issues related to this research and shares insight into the research questions. The review critically discusses CC by looking into different definitions of CC. Furthermore, this chapter discusses the related technologies, service models, major cloud service providers and their cloud offerings, types of CC, benefits of CC and factors that influence organisations CC readiness. This chapter also presents CC in relation to financial institutions by discussing the benefits of CC to financial institutions, common uses of CC by financial institutions and CC risks for financial institutions. A general overview of CC in SA will also be discussed in this chapter. Readiness and what it means in the context of this research will also be discussed in this chapter. Various factors that need to be considered by organisations before moving into the cloud are also discussed in this chapter. The final section of this chapter present a three step change management process proposed by Kotter & Schlesinger, (2008) which is necessary in order to successfully manage the changes that will arise during CC implementation.

2.1 Cloud computing

Every organisation need to begin to find out where CC is needed in their organisation to remain competitive. A unique characteristic of CC is that it is based on a pay per use model which allow companies to pay for services on demand (Goldstuck, 2011; Misra & Mondal, 2011; Yeo, Venugopal, Chu, & Buyya, 2010).

2.1.1 What is cloud computing?

The National Institute of Standards and Technology (NIST) defined CC as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Zhang, Cheng, & Boutaba, 2010; Canedo, de Sousa Junior, & de Oliveira, 2012). It should be noted that this definition by NIST was based on access and availability of resources. Islam and Gregoire, (2012) defined CC as a collection of applications, hardware and system software designed to deliver services to end users over the Internet. Islam and Gregoire, (2012)'s definition focuses on Software as a Service (SaaS) as it is concerned with the delivery of services to the end users. Kshetri, (2010) defined CC as a model in which companies can access computing power and resources on the cloud and pay for services, platform, and/or infrastructure based on usage. Kshetri, (2010)'s definition focuses on the Infrastructure as a Service (IaaS) as it is concerned with the platform and infrastructure that will

enable organisations to develop their own applications and software. Another definition of CC by Khorshed, Ali, & Wasimi, (2012) is that CC is a system, where the resources of a data centre is shared using virtualization technology, which also provide elastic, on demand and instant services to its customers and charges customer usage as utility bill. Khorshed, Ali, & Wasimi, (2012)'s definition can also be said to focus on IaaS as it focused on how the resources of data centre is shared among users. Figure 1 is Schematic definition of CC adopted from Khorshed, Ali, & Wasimi, (2012).

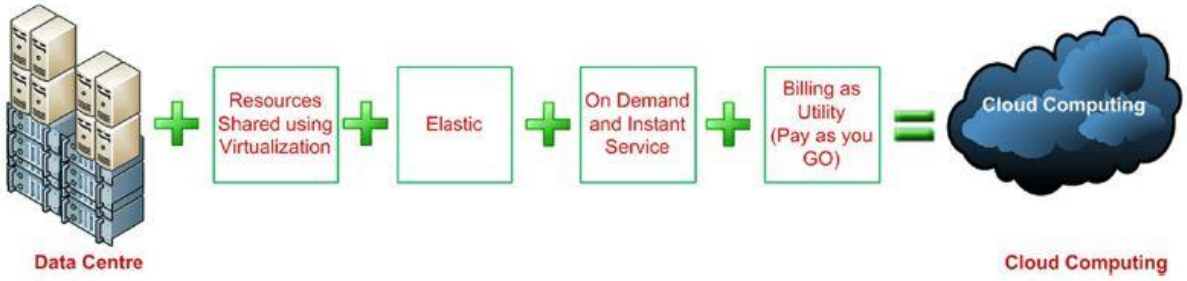

Figure 1: Schematic definition of cloud computing (Khorshed, Ali, & Wasimi, 2012, pg 834)

From the four definitions of CC above, the definition from NIST has been chosen by the authors as working definition for this research because it is more comprehensive and caters for the three main cloud delivery models which are SaaS, PaaS and IaaS (Misra & Mondal, 2011). Following is an explanation of the three cloud delivery models.

2.1.2 Cloud delivery models

The cloud delivery models are built on modern data centres that incorporate SaaS, PaaS and IaaS and provide them as utilities by allowing users to pay per use. Data centres provide the hardware in which the clouds run on and they form the foundation of the cloud. Data centres are usually made up of many servers connected to one another and are located in densely populated areas where there is little chance of a natural disaster. We would now discuss each of the delivery models in details.

It is important to note that the lines that separate the delivery models in figure 2 do not signify a distinction among them. It is possible to find the components and features of one layer in another layer (Tsai, Sun, & Balasooriya, 2010). For example, data storage service can be found in IaaS or PaaS. Figure 2 does not suggest that the layers can only be arranged as shown. For example, it is possible to build a SaaS application directly on top of either IaaS or PaaS. In CC, all the cloud offerings are regarded as a service. Figure 2 shows the hierarchical view for CC and some examples of cloud offerings that can be regarded as a service.

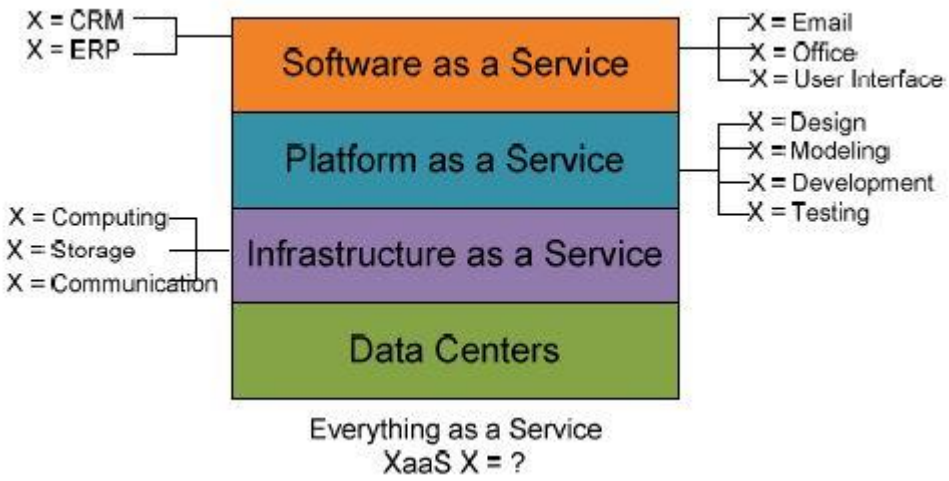

Figure 2: Hierarchical view of cloud computing (Tsai, Sun, & Balasooriya, 2010, pg. 1)

2.1.2.1 IaaS

IaaS is built on top of the data centre layer. It uses virtual machines to provide consumers with storage, networks, processing power, and other important computing resources which allow the consumer to deploy and run their applications and software. A good example is Amazon Elastic Compute Cloud (EC2) service (Maurer, Emeakaroha, Brandic, & Altmann, 2012, Zissis & Lekkas, 2012). With IaaS, the user is able to monitor and control the use of the operating systems, storage, applications, and is also able to exercise a limited level of control over selected networking components (Zissis & Lekkas, 2012). CC is also classified into private, public, community and hybrid cloud based on the deployment model (Zissis & Lekkas, 2012). The major vendors that offer IaaS are Amazon EC2, Amazon S3, Rackspace Cloud Servers and Flexiscale (Ahmed, Chowdhury, Ahmed, & Rafee, 2010). Following will be a discussion on the major cloud service providers.

2.1.2.2 PaaS

PaaS is also known as the cloudware. It provides the consumer with the capability to create their own services and applications with the support of services, programming languages and tools supported and provided by the platform provider (Zissis & Lekkas, 2012; Maurer, Emeakaroha, Brandic, & Altmann, 2012). It does not require software download or installation and it supports collaboration among teams in different locations (Tsai, Sun, & Balasooriya, 2010). Examples of PaaS are Application Engine from Google, Sun N1 Grid, force.com from Salesforce.com, and Microsoft Azure (Ahmed, Chowdhury, Ahmed, & Rafee, 2010; Maurer, Emeakaroha, Brandic, & Altmann, 2012).

2.1.2.3 SaaS

SaaS allows the user to be able to use applications running on a cloud infrastructure from a provider without having to worry about the management or control of cloud infrastructure such as servers, storage, network, operating systems, storage, and other infrastructure that supports CC (Zissis & Lekkas, 2012). The service provider is solely responsible for any update or change in the application (Wang, Rashid, & Chuang, 2011). Major vendors of SaaS are Google Apps and Salesforce.com (Maurer, Emeakaroha, Brandic, & Altmann, 2012). Examples of SaaS are gmail, google maps and Google docs from Google, Hotmail and Business Productivity Online Standard Suite (BPOS) from Microsoft (Ahmed, Chowdhury, Ahmed, & Rafee, 2010; Tsai, Sun, & Balasooriya, 2010).

2.1.3 Related technologies

CC has derived some of its characteristic from earlier technologies which are similar to it. Some of these technologies are grid computing, virtualization and autonomic computing. We would now discuss of each of these technologies in detail:

2.1.3.1 Grid computing

Grid computing is a distributed computing that allows infrastructure on a network to be shared across several organisations in a coordinated manner in order to perform computational objectives (Zhang, Cheng , & Boutaba, 2010). One of the similarities between CC and grid computing is that they both aim to achieve resource virtualization (Dillon, Wu, & Chang, 2010). Another similarity is that they both accomplish objectives at the application-level using distributed resources (Zhang, Cheng , & Boutaba, 2010). One of the differences between CC and grid computing is that grid puts emphasis on resource sharing while CC to form a virtual organisation while CC can be owned by a single organisation i.e. private cloud. Another difference is that CC offers on-demand computing and allows users to sale up or down depending on their needs while grid computing offers maximum computing (Dillon, Wu, & Chang, 2010).

2.1.3.2 Virtualization

This involves the setting up of independent virtual machines (VMs) that are isolated from the underlying hardware and other VMs (Dillon, Wu, & Chang, 2010). These virtual machines provide virtualised resources for high-level applications without showing any details of the physical hardware (Zhang, Cheng , & Boutaba, 2010). The foundation of CC is built on virtualisation due to its ability to

provide shared computing resources from various interconnected servers and assign or reassign virtual resources dynamically to applications on-demand (Zhang, Cheng , & Boutaba, 2010).

2.1.3.3 Autonomic computing

Autonomic computing aims at building computing systems that can self-manage changes in service requirements to meet new and existing service demands without human intervention (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2008; Zhang, Cheng , & Boutaba, 2010). Both CC and autonomic computing have the capabilities of automatic resource provisioning but one significant difference between them is that CC aims to reduce cost while autonomic computing aims to reduce systems complexity (Zhang, Cheng , & Boutaba, 2010).

In summary, CC has similarities with related technologies such as grid computing, utility computing, virtualization and autonomic computing. Since CC has a combination of features from most of the related technologies, CC promises more benefits than them.

2.1.4 Major cloud services providers

Table 2 is a list of the major cloud services providers in the market. The table shows the three main cloud delivery models, the providers, and an example of the specific cloud offering from each provider. Organisations will need to familiarise themselves with the different service providers and their cloud offerings in order for them to be able to choose the most appropriate cloud offering and provide for their business needs. A more comprehensive list of Service providers and the type of services they offer can be found in Appendix E. It is important to note that the list in appendix E is arranged alphabetically and is not based on rankings. The following section will discuss the different types of cloud in details.

	Service Type	Providers	Example
1	**Software as a Service (SaaS)**	Salesforce.com Google NetSuite Apple	Sale Cloud Google Docs NetSuite CRM+ iCloud
2	**Platform as a Service (PaaS)**	Google Microsoft Salesforce	Google Apps Azure Force.com
3	**Infrastructure as a Service (IaaS)**	Amazon Savvis GoGrid	Amazon Services Colocation hosting Cloud Hosting

Table 2: Major cloud services providers (Wang, Rashid, & Chuang, 2011, pg. 239)

2.2 Types of cloud computing

Selecting the right type of cloud to implement is an important step for organisations to successfully implement CC because different types of cloud require different resources and expertise. Most organisations that have failed in their CC implementation failed due to selection of a wrong cloud (Chauhan, Bansal, & Alappanavar, 2012). Organisations need to carefully analyse their data to decide which type of cloud to implement to avoid implementation failure. The different types of cloud are discussed below.

2.2.1 Private cloud

This type of CC requires organisations to have their own servers which may be managed by the organisation or an appointed third party (Ghanbari, Simmons, Litoiu, & Iszlai, 2012). The servers may exist on the organisations premises or on the third parties premises but they are dedicated to a particular organisation (Ahmed, Chowdhury, Ahmed, & Rafee, 2010; Zissis & Lekkas, 2012).

2.2.2 Public cloud

In a public cloud infrastructure, the servers and other resources are owned by a third party service provider who makes the resources available to the general public (Zissis & Lekkas, 2012). The server and all other resources are shared among the organisations and they are billed per usage (Zissis & Lekkas, 2012). An example of public cloud is Amazon Elastic Compute Cloud (Amazon EC2) (Wang, Rashid, & Chuang, 2011). In a public cloud, the user has no control over where the infrastructure is located as the infrastructure is located on the service provider's premises (Ahmed, Chowdhury, Ahmed, & Rafee, 2010).

2.2.3 Community cloud

The cloud infrastructure is shared among several organisations within a community with certain communal goals (Zissis & Lekkas, 2012). The infrastructures may be managed by the organisations or a third party (Zissis & Lekkas, 2012).

2.2.4 Hybrid cloud

In hybrid cloud, the infrastructure is made up of a combination of two or more types of cloud (Zissis & Lekkas, 2012). This type of cloud infrastructure is very efficient in a situation where an organisation has data which is separated into sensitive and non-sensitive data (Wang, Rashid, & Chuang, 2011). The sensitive data could be stored on the private cloud for better control by the organisation while the non-sensitive data could be stored on the public cloud (Wang, Rashid, & Chuang, 2011). Figure 3 is a diagrammatic representation of the four types of CC.

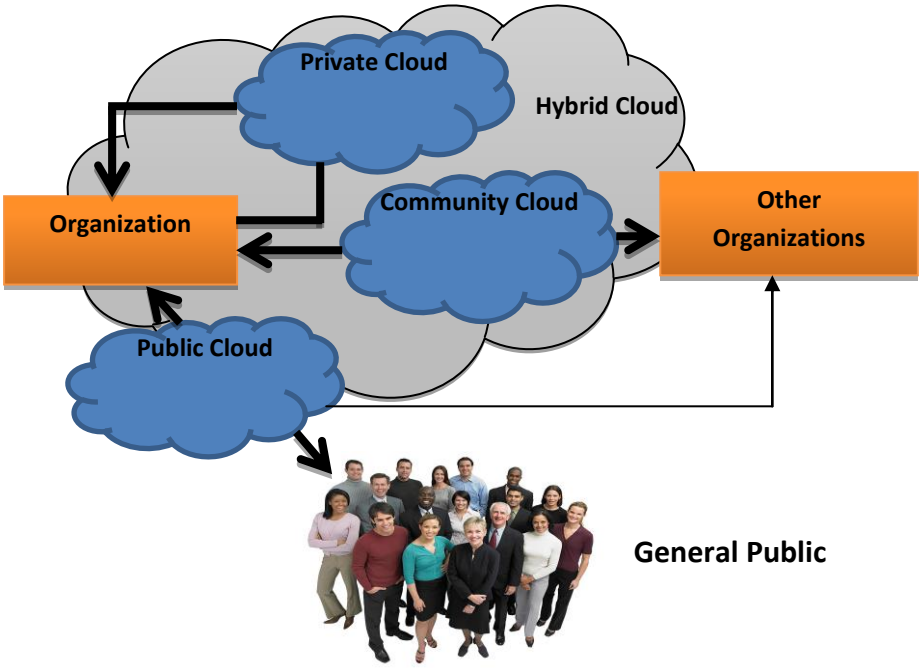

Figure 3: The cloud computing deployment models (Kuo, 2011, pg 4)

2.3 Benefits of cloud computing

CC offers a lot of benefits which can turn around the way organisations do their business and improve their business processes. Some of the key benefits of CC will be discussed below.

2.3.1 Scalability and flexibility

The scalability and flexibility of CC is one of the factors attracting organisations to CC. Cloud architecture can easily be scaled up or down depending on demand because it is easy to add a new node or server to the cloud network in case of high demand (Wang, Von Laszewski, Kunze, & Tao, 2010; Zissis & Lekkas, 2012). When the demand is low, a node or server can also be removed from the cloud network without any negative effect on the efficiency of the network (Zissis & Lekkas, 2012).

2.3.2 Broad network access

CC infrastructure can be assessed over a wide range of networks from smart phones, laptops, and ipads etc. (Zissis & Lekkas, 2012).

2.3.3 Pay per use

CC provides on demand resources and services for users who only pay for services or resources used (Wang, Von Laszewski, Kunze, & Tao, 2010). This will assist the users to maximise their resources and yield better outcomes from their resources as they only pay for what they use.

2.3.4 Economies of scale and cost effectiveness

In the past, organisations have had to buy their own hardware and software to automate and improve their business processes (Wang, Rashid, & Chuang, 2011). Information Technology (IT) teams were also employed by organisations to manage their hardware and software (Wang, Rashid, & Chuang, 2011). CC implementations have revolutionised as the management of the hardware's and software's is now the responsibility of the third party service provider (Wang, Rashid, & Chuang, 2011). CC implementation have been found to be cost effective as it help organisations to eliminate the cost of buying, installing, maintaining and upgrading hardware and software, and allow companies to pay for services on demand (Goldstuck, 2011).

2.3.5 Reliability

The consistent availability of multiple redundant sites improves the reliability of CC and makes it efficient for disaster recovery planning and business continuity (Zissis & Lekkas, 2012).

2.3.6 Increases speed of time to market

CC can provide a quick access to infrastructure, services, or platform that will help organisations speed up their business processes and lead to a faster time to market (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

2.3.7 User centric interfaces

The cloud interface does not require users to change their working habit and environments like programming language and operating systems. This differentiates CC from Grid Computing as users are forced to learn grid commands and application programming interfaces (APIs) to access grid resources and services (Wang, Von Laszewski, Kunze, & Tao, 2010). Cloud interfaces are independent of location and can be assessed from anywhere via interfaces such as web services framework and internet browser (Wang, Von Laszewski, Kunze, & Tao, 2010). The Cloud client software e.g. Nimbus Cloudkit client which is installed on the clients system is only fifteen megabytes (15MB) which does not take up the clients storage space (Wang, Von Laszewski, Kunze, & Tao, 2010). It is important to note that although CC offers a lot of benefits, it also present its users with some issues which prevents many organisations from moving into the cloud. The following section will discuss some of these problems and issues in more depth.

2.4 Issues with cloud computing

The lack of frameworks or methodology to guide organisation in their CC implementation makes it difficult for many organisations to successfully implement CC (Nasir & Niazi, 2011). Before implementing CC, organisations should carefully investigate the perceived failures of CC projects and why those projects fail as part of the steps towards CC readiness (Chauhan, Bansal, & Alappanavar, 2012). Some of the issues that prevent organisations from adopting and implementing CC include uncertainty about availability, fear of vendor/data lock in, uncertainty about data confidentiality, cost, integrity issues and poor band width. The following section will discuss these issues in detail.

2.4.1 Security

Security involves confidentiality, privacy, integrity and availability which aid the development of secure systems. There is so much concern about security within CC environment (Zissis & Lekkas, 2012). Literature has revealed that security is the biggest management issue with CC (Zissis & Lekkas, 2012) because applications and data being hosted by service providers are prone to vulnerabilities from unauthorised parties (Carroll, Van der Merwe, & Kotzé, 2011). Security measures should be taken to prevent unauthorised access to data, applications, software, and hardware. In CC, security is not guaranteed because business information and critical IT resources are outside the company firewall on the service provider's premises (Rao, Nazeer, Rani, & Krishna, 2011). This is a major concern for organisations before adopting CC.

2.4.1.1 Confidentiality and privacy

Confidentiality means that only an authorised person will have access to data. In CC, the chances that data will be accessed by an unauthorised person are increased as a result of many users using the same resources such as memory, networks, data, and programs (Teneyuca, 2011; Zissis & Lekkas, 2012). The fear that confidential and sensitive organisational data might be loss or exposed to third party as a result of the increased number of parties, devices and applications on the cloud is another reason why organisations are reluctant to adopt CC (Armbrust, et al., 2009, Zissis & Lekkas, 2012). CC uses a business model that shares resources such as memory, networks, data, and programs among different users (Teneyuca, 2011). These could lead to breach of data confidentiality as current data retention strategies over the internet platform have been found to be inefficient (Teneyuca, 2011). There have been issues of unauthorized access to user accounts as a result of weak access control and application programming interface (API) infrastructures (Teneyuca, 2011). The issue of data loss and leakage is of major concern to organisations in implementing CC.

Privacy means that control of disclosure of personal information lies with the information owner (Zissis & Lekkas, 2012). Privacy is a serious management issue with CC because data might be saved in numerous locations within a country or even in different countries which poses a bigger risk of confidentiality and privacy breach (Zissis & Lekkas, 2012). Another problem with this issue is that there are legal challenges towards privacy issues involved in data stored in the cloud across different countries because each country have their own laws and jurisdiction regarding confidentiality and privacy (Zissis & Lekkas, 2012).

2.4.1.2 Integrity

Integrity means only an authorised person can make changes to data, software, and/or hardware (Zissis & Lekkas, 2012). The uncertainty about integrity is another problem that prevents organisations from adopting CC (Zissis & Lekkas, 2012). Because of the increased number of users sharing the same resources on the cloud, it is important for service providers to maintain data integrity and accuracy to increase organisational confidence in CC (Zissis & Lekkas, 2012). In a situation where where an employee who is unhappy decides to delete or make unnecessary changes to data, it may be difficult to identify the perpetrator as fingers might be pointed to the service provider (Zissis & Lekkas, 2012). Authentication can help resolve this issue as the user with such permissions can easily be identified. It is also very difficult for an organisation to check the data handling practices of the cloud service provider and confirm that their data is being handled in a lawful way (Khajeh-Hosseini, Greenwood, & Sommerville, 2010). Service providers need to make their data handling process transparent to the customer organisations to gain their trust.

2.4.1.3 Availability

Availability refers to the service, data, and infrastructure being accessible to authorised users immediately upon request (Armbrust, et al., 2009; Zissis & Lekkas, 2012). Organisations need to be assured that there will be an uninterrupted access to service, data, and infrastructure without interruption even in the event of a security breach (Zissis & Lekkas, 2012). Since there is no guarantee for continuous availability, many organisations are reluctant in moving their data into the cloud and do not make further effort to get themselves ready for CC adoption. An example is that of Salesforce.com in 2009, when they had a major outage in which 900,000 subscribers were unable to access important information in time (Wang, Rashid, & Chuang, 2011).

2.4.2 Data lock in

Organisations are reluctant to adopt CC because of concerns over data lock in due to lack of standards (Armbrust, et al., 2009; Maurer, Emeakaroha, Brandic, & Altmann, 2012; Rodero-Merino, et al., 2010). The fear of uncertainty such as the provider going out of business, price increases, and reliability issues as a result of data lock in also prevent organisations from adopting CC (Armbrust, et al., 2009)

2.4.3 Jurisdictional issues

It is often difficult to fix resources such as data centres to a specific geographic location (Hay, Nance, & Bishop, 2011). Load balancing by the cloud provider, network availability, and data centre performance are some of the factors that determines where a data is stored (Hay, Nance, & Bishop, 2011). As a result, an organisations data may be stored in different locations with different legal jurisdictions and different laws about security issues such as data protection and intrusions (Hay, Nance, & Bishop, 2011). This is an important issue for organisations to consider before adopting CC as the safety of their data is eminent for the continued success of the organisation.

2.4.4 Lack of standardised service level agreement

Although SLAs exists, there are different SLAs in CC market because of the different definitions of CC resources which are often described through different non standardised resources such as execution time, inbound bandwidth, outbound bandwidth, central processing unit (CPU) cores, and processor type (Maurer, Emeakaroha, Brandic, & Altmann, 2012). The lack of standardised SLAs is an issue that hinders wide adoption of CC (Tsai, Sun, & Balasooriya, 2010). There is a need for service providers and users to standardise SLAs that will guide their business relationship and help to ensure delivery of agreed resources. Organisations need to ensure that there is standardised SLA between the service provider and the organisation to ensure delivery of agreed service.

2.4.5 Customisation

The sharing of resources by differing users prevents service provider from being able to customise their services to suit the different customer needs (Joint & Baker, 2011).

Customisation affects CC readiness of organisations because most organisations are uncertain about CC customisability to meet their specific business needs (Joint & Baker, 2011). Wang, Von Laszewski, Kunze, & Tao, (2010), however share a different view as they believe that users can customise and personalize their computing environments like software installation, and network configuration. Organisations will therefore need to find out more about the resources and services that can be customised to their business needs to ensure that CC will offer such customisation before implementing CC.

2.4.6 Lack of flexibility for user interface

User Interface composition frameworks have not been integrated with CC and this has a great influence on user experience which is an important factor in assessing an application before adoption (Tsai, Sun, & Balasooriya, 2010).

2.4.7 Decrease in job satisfaction

CC may lead to a decrease in job satisfaction of support engineers, support care staff , and sales and marketing staff as most of the technical roles will be taken up by third party service provider and support engineers will only be left to do some reporting work and resolving issues with third party service providers (Khajeh-Hosseini, Greenwood, & Sommerville, 2010). The fear that CC will reduce the work of employees and possibly make some employees lose their jobs affects organisations CC readiness because employees will not make efforts to get the organisations ready for CC because of the fear of losing their jobs to a third party service provider (Khajeh-Hosseini, Greenwood, & Sommerville, 2010).

2.4.8 Lack of supporting resources

Migration to the clouds requires knowledge and experience from the organisations support engineers. The implementation of a new technology requires knowledge about its existence and its applicability (Heinle & Strebel, 2010). Lack of prior knowledge and experience of CC by the support engineers can be very risky for the organisation (Khajeh-Hosseinil, Greenwood, & Sommerville, 2010). Organisations need to ensure that they have the right skills and expertise require for CC because CC is a technical area that requires skilled resources for implementation (Chauhan, Bansal, & Alappanavar, 2012).

2.4.9 Service provider selection

Because of the different CC service providers, organisations find it difficult in choosing a service provider. While choosing a service provider, organisations should consider factors such as the reputation and size of the service provider's organisation in terms of staffs, market share, as well as their resources (Heinle & Strebel, 2010).

The process of choosing a service provider is very important because if the organisation chooses a wrong service provider, the cost of moving from one provider to another can be high due to incompatible programs (Vignos, Kim, & Metzer, 2013).

Organisations need to be aware of the different service providers and how their offerings fits with their requirements as this influences organisations decision on CC, which will in turn affect their level of readiness and ultimately the success of their CC adoption.

2.4.10 Technological bottlenecks

CC requires organisations to upgrade their existing technology in terms of new data structures so as to be able to handle dynamic and large amounts of data, new file systems, and storage technologies (Goel, Kiran, & Garg, 2011). The organisations should involve their IT department in their CC to assist them in their CC readiness because most organisations fail in their CC implementation because their business department is concerned with their time to market demands and as a result, the IT department is not given the chance to investigate the organisation CC readiness (Chauhan, Bansal, & Alappanavar, 2012).

2.4.11 Strategy issues

The introduction of CC will bring about a change in the organisations information technology (IT) structure (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). Some of the questions that need to be answered to resolve the strategy issues are: what type of cultural change does the organisation need, how will the change be addressed, and how will the organisation prevent employee resistance of CC (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). One of the possible changes in the IT structure due to the introduction of CC could be the downsizing of IT department as most of the work done by the IT department will now be done by the service providers (Khajeh-Hosseini, Greenwood, & Sommerville, 2010). This can also lead to a decrease in job satisfaction of technical staffs, support care staff , and sales and marketing staff as most of the technical roles will be taken up by third party service provider and technical staffs will only be left to do some reporting work and resolving issues with third party service providers (Khajeh-Hosseini, Greenwood, & Sommerville, 2010). This is a sensitive issue because employees may not accept CC because of the fear of losing their job or being reduced to support personnel whose job will be to log complaints to the service provider (Khajeh-Hosseini, Greenwood, & Sommerville, 2010). The question of whether the organisation has skilled IT professionals with experience to manage CC is also an important strategic issue (Lin & Chen, 2012). The effect of CC on organisation culture and how well the management is able to address this issues and convince the employees to accept CC will be influential in determining the success or failure of their CC implementation (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

2.4.12 Change management

The implementation of CC brings about a change in the way organisations carry out their daily activities. The process of change management is therefore a serious management issue because it will determine the success of the organisations CC implementation (Carroll, Van der Merwe, & Kotzé, 2011). Proper change management practices should be put in place in order to overcome issues as a result of change.

Implementation issues are also important as the success of implementation will bring about the desired change through CC. Implementation issues will be discussed in the following section.

2.4.13 Implementation issues

Organisations find it difficult to determine which of their data should be moved into the cloud and which should remain on the organisations traditional system (Khajeh-Hosseini, Greenwood, & Sommerville, 2010). Organisations are also concerned about how to migrate their data into the cloud without any interference in their businesses during migration. Organisations are also faced with the issue of how to integrate their traditional in-house applications with cloud applications (Khajeh-Hosseini, Greenwood, & Sommerville, 2010).

2.4.14 Reputation fate sharing

The problem of reputation fate sharing arises when one organisation sharing the same resources with other organisations has a bad reputation and this affects other organisations (Roberts II & Al-Hamdani, 2011). This is a major issue because organisations will not like the activities of other organisations to affect them as they have their own integrity to protect. An example of reputation fate sharing was when the FBI agents in Unites states raided a data centre because there was a suspected cybercrime being committed from hardware in the data centre (Roberts II & Al-Hamdani, 2011). Because of that, the operations of all the organisations sharing that data centre was halted during the period that the FBI agents were looking for evidence for the cybercrime case. Another important issue is CC's dependent on the internet. This issue is discussed in details below.

2.4.15 Dependence on internet

The dependence of CC on the internet is a serious management issue because if there is any problem with the internet, CC will be affected. CC depends on internet to function properly (Roberts II & Al-Hamdani, 2011). If there is no internet connection, it automatically means CC cannot function. Slow internet connections will also affect service delivery of CC (Chauhan, Bansal, & Alappanavar, 2012). In order to resolve this issue, customer organisations should endure they subscribe to a reliable internet service provider who will guarantee consistent, fast and reliable internet connection. Organisations can also have back up internet connections like wireless connections which they can automatically switch to when their main internet connection is down.

2.4.16 Integration issues

Organisations prefer to implement the hybrid model in order to have control over their important and sensitive data and infrastructure (Canedo, de Sousa Junior, & de Oliveira, 2012). The less sensitive data is then migrated to a public cloud. Management find it difficult to integrate their in-house infrastructure and service provider's infrastructure because of the different API's which makes the infrastructure incompatible (Armbrust, et al., 2009). Standardisation of API's will also help resolve these issues. Malicious insiders, risk management, and performance measurement which are also important issues with CC are discussed in the following sections.

2.4.17 Malicious insiders

An employee of the service provider may also cause a security breach because the employee may have access to confidential data and services which may then be exposed to unauthorised third parties. This is a serious issue for service providers because they have an ethical duty to protect customer data (Khorshed, Ali, & Wasimi, 2012).

2.4.18 Risk management

CC exposes organisations to a wide range of risks. The management of these risks is a serious issue because the success of CC implementation depends on proper management, reduction, and mitigation of risks associated with CC (Dorey & Leite, 2011). The following section will discuss the benefits, risks, and common uses of CC by financial institutions.

2.5 Financial institutions and cloud computing

CC adoption rate of financial institutions is low because of issues such as security, loss of control over data, data privacy, lack of standard SLA's etc. that are documented in literature. The fear that the financial institution will be dependent on the service provider is another reason why financial institutions have been slow in the adoption of CC (Howell-Barber, Lawler, Desai, & Joseph, 2013).

Although the adoption of CC by financial institutions has been slow, CC is not new to financial institutions. Many financial institutions have adopted some form of CC but they have been selective in their choice of CC because of the concerns about CC. The earlier form of CC adopted by financial institutions was SaaS which was used for social media banking (Sharma, 2012). Other CC services used by financial institutions include collaboration, CRM systems, desktop and e-mail systems (Howell-Barber, Lawler, Desai, & Joseph, 2013).

In order to maximise the benefits of CC, financial institutions need to select the right operating, service, and deployment models to resolve security and compliance issues.

2.5.1 Benefits of cloud computing to financial institutions

Many financial institutions are already using CC while others are seriously considering moving into the cloud. CC offers facilities such as email, web hosting and fully managed applications which enhances communication between financial institutions and clients (Sharma, 2012).

CC provides financial institutions with the opportunity to outsource their IT operations and infrastructure to a third party service provider, and be able to concentrate on their business and not IT. With service level agreements (SLAs) in place, service delivery and availability are assured by cloud providers. CC also helps to reduce risk management costs as well as operational risk (Agopyan, Sener, & Beklen, 2010).

CC provides financial institutions with the opportunity to scale up or down depending on demand from customers thereby enabling them to save on the cost of acquiring and maintaining the resources that are not needed (Sharma, 2012).

Performance of financial institutions can be increased by CC in a number of ways. Firstly, CC allows financial institutions to avoid large upfront cost and allows them to select services and applications that they need and pay based on usage (Sharma, 2012). A higher level of fault tolerance, data

protection, and disaster recovery can be achieved by financial institutions because the responsibility of managing CC lies with the service provider.

CC can also reduce product development cycle of financial institutions because of the time it helps to save by eliminating the need for purchase, installation, and maintenance of infrastructure which saves time. This allows financial institutions to reduce their focus on IT and pay more attention to their business thereby allowing them to attend to their customers' needs in a timely manner (Sharma, 2012).

2.5.2 Common uses of cloud computing by financial institutions

Many financial institutions use CC for customer relationship management (CRM) and Customer analytics (Sharma, 2012). CC helps to improve customer satisfaction because it facilitates sales, customer engagement, interactions and servicing. CC also improves customer satisfaction because it allows staffs to have quick access to information which helps them in answering customers' questions effectively and on time (Sharma, 2012).

2.5.3 Cloud computing risks for financial institutions

One of the risks of CC that financial institution needs to consider is constant dependence on internet. Any problem with the internet would lead to interruption of CC services and this could be costly for financial institutions especially in departments such as exchange rate departments where real time information is needed (Sharma, 2012). There might be problems when moving applications across from one service provider to another as the service provider is responsible for backup and recovery of data (Sharma, 2012).

Legal issues are also important for financial institutions to consider as to who owns the data and who is allowed to access data. For example, in cases where there is a court order or government officials demand to access data to conduct investigations, several legal issues arise and it is important for financial institutions to know how to handle such situations in order to retain the trust their customers have in them (Sharma, 2012).

Finally, customer information and financial information about transactions are important to financial institutions. Data should be protected from leakage, intentional or accidental loss to protect the reputation of the institution and increase customer's confidence (Sharma, 2012).

In order to understand CC in the context of SA, the following section will discuss CC in SA.

2.6 Cloud computing in South Africa

CC is growing in SA and most organisations in SA have already adopted one form of CC or the other (Hinde & Van Belle, 2012; Kshetri, 2010). More and more SA organisations are adopting CC to reduce cost (Goldstuck, 2011). Google was rated as the most credible vendor in SA and the cloud services mostly used in SA were webhosting and e-commerce, email hosting/archiving, customer relationship management Systems (CRM), configuration and data backup, and application development (Hinde & Van Belle, 2012).

In 2009, IBM built a data centre in Johannesburg to offer cloud services to SA organisations and Vmware also launched vSphere's, a cloud OS in 2009 to serve SA market (Kshetri, 2010). There has been a considerable improvement in SA's bandwidth in recent years (Mahlong, 2012). SA's bandwidth issues are improving because new undersea telecommunications cables are being developed to increase bandwidth availability in SA (Grobler & Dlamini, 2010). The overall online activity of SA was estimated to be 67% of the combined online activity of all African countries. SA is ranked as one of the top internet countries in Africa and this is good news for CC as it means the quality of internet services available to support CC will be fine (Grobler & Dlamini, 2010).

Over twelve million cell phone users in SA are said to have internet connectivity on their phones (Grobler & Dlamini, 2010). This means that the cloud services of financial institutions can be accessed by customers via the internet enabled phones and it will contribute to customer satisfaction and assist financial institutions to reach more customers than they would have been able to reach without the technology (Grobler & Dlamini, 2010).

In terms of security attacks over the internet, in 2010, SA had at least 4646 reported incidents of cybercrime which led to a direct financial loss of $573 million and an extra $995.4 million in time spent to resolve the crime (Grobler & Dlamini, 2010). Financial institutions in SA need to be aware of these crimes and how to combat them in order to gain the trust of their customer and ensure a successful implementation of CC (Grobler & Dlamini, 2010). Although cybercrime is said to be high in SA, that should not prevent financial institutions from adopting CC as there are many security measures in place to protect data and prevent cyber-attacks in CC (Rani & Gangal, 2012).

Following on from here will be a discussion on readiness and a definition of readiness in the context of this research.

2.7 What is readiness?

Readiness means different things to different people, in different contexts, and for different purposes. (Vaidya, Sajeev, & Gao, 2005) defined readiness as the availability of needed organisational resources to adopt a technology. Fathian, Akhavan, and Hoorali, (2008) defined readiness as the ability of an organisation to successfully adopt, use, and benefit from a technology. The definition from Fathian, Akhavan, and Hoorali, (2008) and Vaidya, Sajeev, & Gao, (2005) has been selected as the working definition for this research. As a result, it is important to define CC-readiness in the context of this research based on the selected working definition. CC-readiness of a financial institution means the ability of the financial institution to successfully adopt, use, and benefit from CC through efficient use of available resources. In order to clearly explain what readiness means in the context of this research, readiness is shown in figure 4 as a stage before adoption.

In order to ensure a successful implementation of CC and properly manage changes that arise as a result of CC, organisations need to prepare themselves and be ready before implementation. This is because "more than half of all unsuccessful large-scale organisational change efforts are as a result of failure to establish sufficient readiness" (Weiner, 2009, pg.1).

Figure 4 is a diagrammatic representation of readiness in relation to adoption. Once an organisation decides to implement CC, the organisation should determine their level of readiness for CC to determine their suitability for a successful adoption. Once the readiness level is known and the organisation CC readiness in good enough, only then can the organisation decide to adopt CC. Some of the factors that organisations should consider to determine their readiness for CC implementation are discussed in greater depth in the following section.

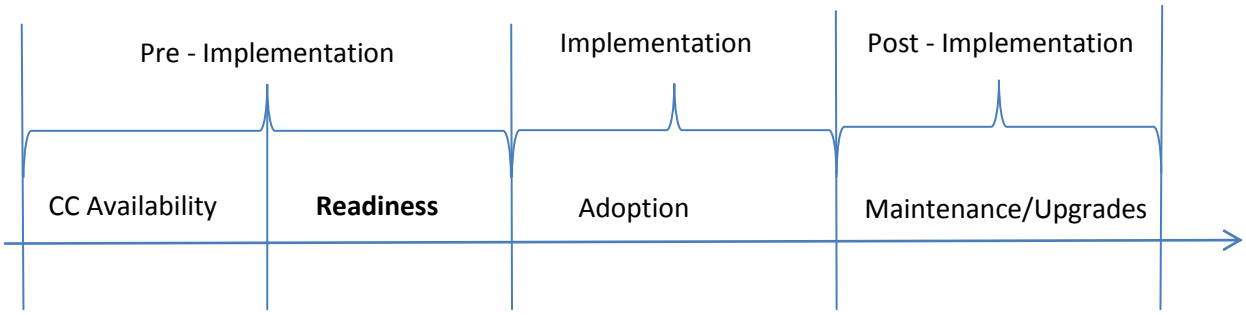

Figure 4: Schematic representation of the differences between readiness and adoption

2.8 Considerations for organisations before moving into the cloud

Misra & Mondal, (2011) noted that the key characteristics of the resources possessed by an organisation to be considered before moving into the cloud include size of the IT resources and the utilization pattern of the resources. Another characteristic is sensitivity of the data they are handling i.e. if their data is mostly confidential, they may prefer to adopt private cloud in which they will be have their own data centre and be in total control of their data instead of the public cloud where the cloud provider will own the data centre and have control over the data. The last characteristic is criticality of work done by the company.

These characteristics must be thoroughly considered by organisations before implementing CC as this will help them to determine what type of cloud services they require. These characteristics have been grouped based on the Technology, Organisation, and Environment (TOE) framework by Tornatzky, Mitchell, & Chakrabarti, (1990) which is the selected framework for this research in order to add a profound theoretical stance to this research.

2.8.1 Technology

2.8.1.1 ICT infrastructure

Organisations should ensure that the entire necessary infrastructure to support CC is available to them before deciding to implement CC. This includes the availability of necessary technologies and expertise to operate those technologies (Carroll, Van der Merwe, & Kotze, 2011).

2.8.1.2 Technology awareness

The knowledge and awareness of an organisation about a technology is important for the success of implementation. If an organisation is aware of a technology, they will be able to make necessary preparations before adoption and this will increase the success of their implementation (Carroll, Van der Merwe, & Kotze, 2011).

2.8.2 Organisation

2.8.2.1 Size of the IT resources

The size of organisations IT resources is important in determining an organisations CC readiness because it will help the organisation to determine which type of cloud to implement (Misra & Mondal, 2011). Organisations with large data centres and large IT infrastructure may decide to implement private cloud for example as this is more secure and the privacy and confidentiality of

their data can be ensured because the organisation will be able to maintain total control of their data. In order to determine the size of the IT resources of an organisation, the number of servers the company maintains in its data centres, the size of the customer base of the company, the annual revenue from IT, and the number of countries across which the company has branches should be considered (Misra & Mondal, 2011).

2.8.2.2 The utilization pattern of the resources

Organisations should determine the utilisation pattern of their resources by considering the average usage and peak usage, and amount of data handling/transactions done (Misra & Mondal, 2011). For example, organisations whose resources are underutilised may need to move into the cloud to cut the cost of maintaining the unused resources and only pay for the utilised resources while on the cloud. This will be of high benefit to organisations because it will allow them to maximise the use of their resources and reduce waste thereby helping them save a lot on cost. Organisations that handle a large amount of data will require a large bandwidth to process and store data in the cloud (Misra & Mondal, 2011). This will mean that the amount of money they will spend on bandwidth will be a lot and it will not be advisable for them as the cost of CC may then be more than the cost of their traditional systems in the long run (Misra & Mondal, 2011).

2.8.2.3 Sensitivity of the data they are handling

Organisations with sensitive and confidential data need to carefully identify which of their data should be moved into the cloud and which should remain on their traditional systems. They could also decide to move the sensitive data into a private cloud and move the less sensitive data into a public cloud (Misra & Mondal, 2011). This will help them ensure the security of their data.

2.8.2.4 Criticality of work done by the company

Highly critical work requires stringent resources, platforms, applications and security (Misra & Mondal, 2011). Highly critical work also demands very stringent service level agreements (SLA's) and since SLA's have not yet been standardised for CC, it is not be advisable for organisations to carry out their critical work on the cloud.

2.8.2.5 Top management support

Support from management is an important factor to consider before implementing CC as the availability of resources for CC implementation depends on the management's decision to make

necessary resources for the implementation of CC available (Al-Somali, Gholami, & Clegg, 2011; Pudjianto , Zo, Ciganek, & Rho, 2011).

2.8.2.6 Satisfaction with existing system

Organisations that are happy with their existing system should not move into the cloud just because it is the latest technology in vogue. They should move into the cloud because of their business needs. Organisations should ensure that they will achieve some improvement in their business process which their existing system is not offering them before deciding to move into the cloud (Carroll, Van der Merwe, & Kotze, 2011).

2.8.2.7 Skills

CC requires some special skills to be implemented successfully. These include negotiation skills and management skills. Organisations should ensure training for their employees to ensure that the employees possess necessary skills to implement CC successfully (McKendrick, 2013).

In order to ensure that CC implementation is successful, there are some necessary skills that organizations must strive to possess at it will help them to properly implement CC to achieve the promises of CC. Regardless of what type of cloud an organization want to adopt, these skills are still needed. For example, with public cloud where most of the computing is done by a service provider, organizations still need to have people with skills to negotiate SLAs, integrate cloud offerings with onsite offerings. They also need to be able to select what services are needed. If the organization decides to implement a private cloud, they will require skills similar to that of service providers as they will have to host and manage the private cloud in-house. CC therefore requires a number of new skills which may require the organization to either train some of their staff in-house or send them to cloud training providers for training in order to equip them with these skills. Some of these skills include:

2.8.2.7.1 Technical skills

It is important to have people that have knowledge of CC infrastructure and architecture. People with programming skills will also be needed to be able to develop cloud applications that can be deployed over the internet in little time. The knowledge of virtualization and all other CC features is also essential (McKendrick, 2013).

2.8.2.7.2 Security

Organizations would require people that know all the necessary security protocols (McKendrick, 2013).

2.8.2.7.3 Compliance

There is also a need for people who knows what laws and regulations are applicable to CC in order to ensure that their organization always acts within the relevant laws and regulations (McKendrick, 2013).

2.8.2.7.4 Project management and change management skills

Organizations need to have people with project management skills who will be able to manage things like time, budget and other resources to achieve the desired goals. They also need to possess change management skills as the implementation of CC would lead to a number of changes in the business processes, IT department and even the entire organizational structure. The ability of CC to allow customers to scale up or down easily require the expertise of people with project management skills, capacity management skills and monitoring tools to be able to decide on what quantity of service is needed so as to avoid paying for what is not needed (McKendrick, 2013).

2.8.2.7.5 Negotiation skills

People with negotiation skills will be of great value to the organization in terms of negotiating the SLA with cloud providers. They will also be able to negotiate with team members in case there any unresolved issues. They also need to be able to negotiate with the cloud providers in case the service goes down or the service provider is not delivering as promised (McKendrick, 2013). They need to possess skills so that will ensure that they are able to resolve the issue with the cloud provider as soon as possible and still maintain a good relationship with the service provider. Ability to negotiate with internal staff is also important to ensure successful internal change management (McKendrick, 2013).

2.8.2.7.6 Business and financial skills

CC also requires the organization to have employees with good business and financial skills. Those employees will be able to develop a business case for CC (McKendrick, 2013). They will also be able

to make informed decision on the type of CC implementation that would benefit the organization in order to get a good return on investment. Finally, they would be able to compare the cost of having the services in-house or in the cloud and be able to decide on which option is more suitable for the organization (McKendrick, 2013).

2.8.2.7.7 Enterprise architecture and business analysis

People with enterprise architecture and business analysis skills are also needed to be able to determine which services are needed by the organization (McKendrick, 2013). They will be able to serve as a link between business and IT in order to gather business requirements needed to decide which type of cloud would be able to meet those business requirements regardless of whether the service is provided in-house or by a third party service provider.

2.8.2.7.8 Data integration and analysis skills

The organization needs people who can integrate the on-premises data with the cloud. Data analysis skills are also important because they will need to determine which data is suitable for the cloud and which one should remain on premises because of issues such as security and privacy in the cloud (McKendrick, 2013). This is important especially for financial institutions that work with sensitive customer information

2.8.2.7.9 Mobile applications development and management

One of the benefits of cloud is that the services can be accessed anywhere and anytime. In order to enjoy this benefit, organizations need to have people who can develop and manage mobile applications (McKendrick, 2013). Some financial institutions in SA have mobile applications which are hosted in the cloud and allow customers to perform transactions such as checking account balance, money transfer and airtime purchase (Goldstuck, 2011). There is a need for people with skills to build and deliver that type of application that can reside in the cloud and be available to staff, customers and business partners anytime and anywhere.

2.8.3 Environment

2.8.3.1 Legislation

Legislation is a very important aspect of readiness as organisations need to be aware of existing laws and legislation about CC. This will ensure that organisations know what to do in case of a breach of SLA, by the service provider. It will also inform organisations on their privacy and information protection. In cases where the data centre is in a different country from the organisations location, the organisations should also be aware of what rights and obligations they have in case of a breach and their information is exposed to a third party.

2.8.3.2 Competition from rivals

Organisations should not simply implement CC because other organisations are implementing CC. Every organisation needs to research and find out how CC could differentiate them from their competitors and improve their business process for increased return on investment. Most organisations that failed in their CC implementation fail because they are not ready for CC as they have little or no technical knowledge about CC (Chauhan, Bansal, & Alappanavar, 2012). Organisations need to have the right motivation for CC and not just do it because others are doing it as this will contribute to the success of their CC implementation.

2.8.3.3 National infrastructure

National infrastructure such as bandwidth, internet facilities and other supporting infrastructures that enables CC should be investigated by organisations so that proper arrangements could be made to ensure that there will be continuous access to the services, infrastructure, and applications subscribed for without any interruptions as a result of poor infrastructure (Al-Somali, Gholami, & Clegg, 2011). Once organisations are sure of the availability of the necessary infrastructure, they can then decide on moving some or all of their data into the cloud.

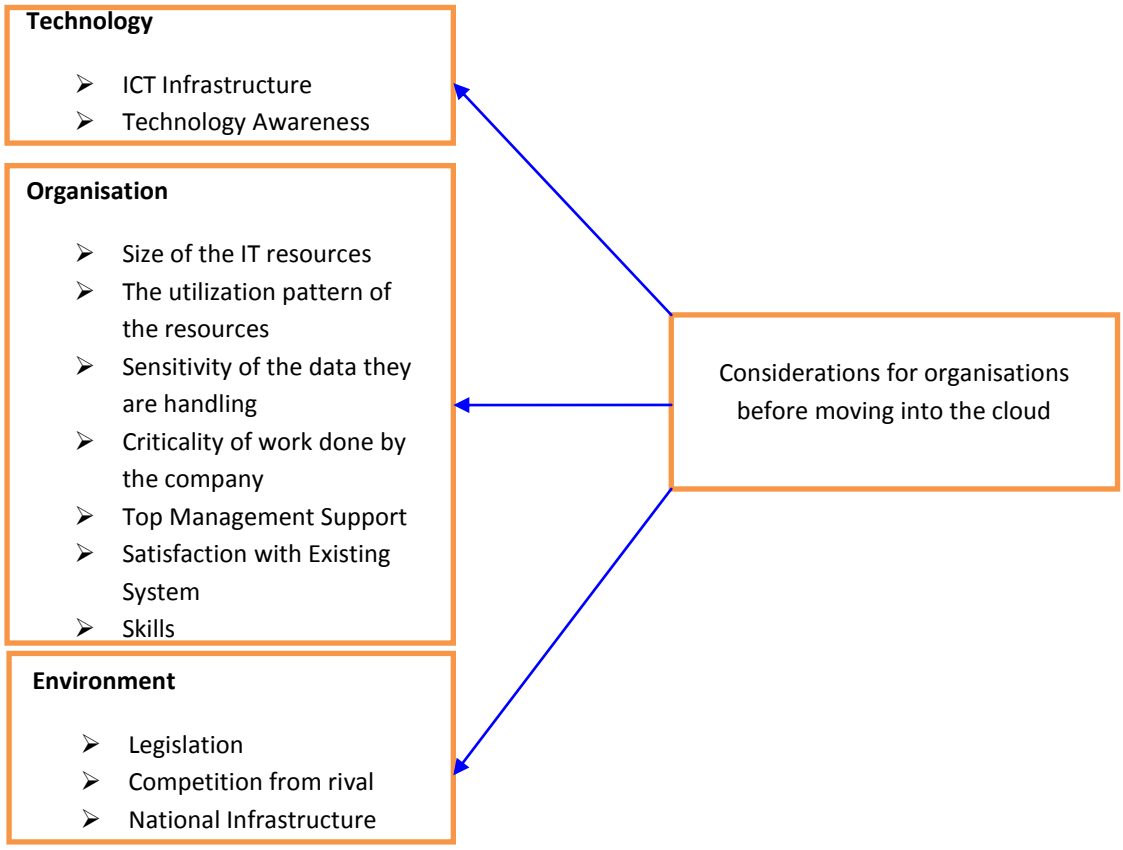

Figure 5: Summary of important factors that organisations need to consider to determine their need for cloud computing using the TOE framework

Implementation of new technologies in organisations sometimes brings a shift in the structure of the organisation. The business processes may also need to be re-engineered. These changes in the organisation need to be properly managed as they could have a negative effect on the implementation process. If the change process is not properly managed, it could also lead to failure of the entire implementation. As a result, an effective change management process needs to be put in place as this will help reduce resistance and other issues that may arise. The following section will discuss the three steps change management process by Kotter & Schlesinger, (2008) as this would be a useful tool in managing the change effectively.

2.9 Change management

The adoption of CC would bring about so many changes in the organisation. This will affect different organisational processes as well as the organisational structure. The impact will be mostly felt by the IT department. These changes will lead to issues such as employee resistance, job insecurity etc. and will affect the adoption of CC (Todnem By, 2005).

In many organisations, when there is a change as a result of technology, the focus is always on the technology and not on managing the changes it brings in the process, structure and culture of the

organisation. The need for change management is only considered if there is a situation of organisational crisis (Benjamin & Levinson, 1993; Todnem By, 2005). This in most cases contributes to the failure in implementation of the technology. As a result it is important for organisations to consider having an efficient change management strategy in place that will assist in ensuring that the changes as a result of adoption neither lead to implementation failure nor affect the organisation negatively.

IT-enabled change processes are different from more general change process because there are some unique issues that arise as a result of IT-enabled change. It is therefore necessary to know how to integrate business process, technology and organisation so that the expected benefits of the technology can be realised (Benjamin & Levinson, 1993).

It is essential for organisations to realise that for the expected benefits of a new technology to be realised, managing the change as a result of the technology is as important as the technology itself (Todnem By, 2005).

In order to manage the change as a result of CC successfully, this research suggests the three steps for managing change successfully by Kotter & Schlesinger, (2008). The three steps will now be discussed in details in the context of change as a result of CC.

2.9.1 Analyse situational factors

The manager or change agent in the organisation needs to analyse the situation by asking himself or herself the following questions:

1. How much and what kind of resistance are we expecting?
2. What's my position in relation to the people who are expected to resist change - In terms of my power and level of trust between me and them?
3. Who has the more accurate information about the changes that are needed?
4. How urgent do we need to implement the change?

Once the manager or change agent is able to provide answers to the above questions, the next step is to determine how urgent the change should be effected (Kotter & Schlesinger, 2008).

2.9.2 Determine the optimal speed of change

The answers to the above questions would assist in determining whether the change needs to happen quickly or slowly. The change should be effected quickly if the organisation is at risk of losing

performance or productivity (Kotter & Schlesinger, 2008). The change can be carried out slowly if resistance will be intense and extensive; if you need information from other people to help design and implement the change; or if you have less power in the organisation than those who may possibly resist the change (Kotter & Schlesinger, 2008).

2.9.3 Consider methods for managing resistance

There are different methods for managing resistance. They can be used individually or alone depending on the situation and the intensity of resistance. The different methods will now be discussed in details.

2.9.3.1 Education

It is important to communicate the desired changes and the reason why there is need for change to everyone across the organisation. This will help reduce resistance as people often feel that they are part of the change and they will be willing to help in implementing change when it is well communicated with them.

2.9.3.2 Participation

The people who are expected to resist the change should be involved in designing and implementing the change. This will also assist in reducing resistance as they would want to be a part of success. It will help to increase their commitment to the change.

2.9.3.3 Facilitation

Necessary arrangements should be made to provide training and emotional support for all the staffs that might be affected by the change in order to provide them with skills which will help them cope with the change.

2.9.3.4 Negotiation

Motivation is the key to ensuring that everyone is committed to the change. Offer incentives for everyone involved in making the change successful. This will improve the chances of success and help the organisation adapt to the changes easily.

2.9.3.5 Coercion

In some instances, when all other approach has failed and employees are bent on resisting the change, even when it has been well communicated to them and incentives are offered. The only alternative left is to threaten them with possible loss of jobs or promotion opportunities. They can

also be informed that whoever is not happy with the change will be transferred to other departments where the impact of the change will be minimal. Although, this method is not the best method and should be used with caution, research has shown that it works quickly and is able to overcome any resistance to change. Table 3 shows the methods involved in step three of the methods for managing change by Kotter & Schlesinger (2013). Each method is discussed based on how to use it, when to you it, advantages and disadvantages.

Method	How to use	When to use	Advantages	Disadvantages
Education	Communicate the desired changes and reasons for them	Employees lack information about the change's implications	Once persuaded, people often help implement the change	Time consuming if lots of people are involved in the change
Participation	Involve potential resisters in designing and implementing the change	Change initiators lack sufficient information to implement the change	People feel more committed to making the change happen	Time consuming and employees may design inappropriate change
Facilitation	Provide skills training and emotional support	People are resisting because they fear they can't make the needed adjustments	No other approach works as well with adjustment problems	Can be time consuming and expensive; can still fail
Negotiation	Offer incentives for making changes	People will lose out in the change and have considerable power to resist	It's a relatively easy way to defuse major resistance	Can be expensive and expose managers to the possibility of blackmail
Coercion	Threaten loss of jobs or promotion opportunities; fire or transfer those who can't or won't change	Speed is essential and change initiators possess considerable power	It works quickly and can overcome any kind of resistance	Can spark intense resentment toward change initiators

Table 3: Methods for managing change (Kotter & Schlesinger, 2008, pg. 1)

The three steps for managing change discussed above will help to ensure that the change process is successful.

2.10 Summary of Chapter

There are three main cloud delivery models which are IaaS, PaaS and SaaS. CC is also classified into private cloud, public cloud, community cloud and hybrid cloud based on the relationship among the users.

The major SaaS providers are Salesforce.com, Google, NetSuite and Apple. The major PaaS providers are Google, Microsoft and Salesforce while the major IaaS providers are Amazon, Savvis and GoGrid. Some researchers have argued that CC is an extension of some earlier forms of computing because of its characteristics which are similar to that of earlier forms of computing such as grid computing, utility computing, virtualization, and autonomic computing. CC also offers benefits such as broad network access, on-demand service provisioning, cost effectiveness, reliability and increases speed of time to market. CC can provide facilities for email, web hosting and fully managed applications which will enhance communications between financial institutions and clients. Another benefit of CC to financial institutions is that it can allow financial institutions to avoid large upfront cost and allows them to select services and applications that they need and pay based on usage. Although financial institutions stand to benefit a lot from CC, they have been slow with the adoption of CC because of issues such as availability, security and privacy, possibility data lock in, data confidentiality, jurisdictional issues etc. which affects their CC readiness. This issues can be resolved through the use of a CC readiness framework that is combined with change management framework as it provide guidance on what to do to get ready and how to manage changes that arise as a result of CC.

3. Research design and methodology

This chapter presents the research methodology by discussing the data collection and analysis as well as the validity of data and framework. The duration of the interviews, profile of participants, role of participants in IT decisions, the participants understanding of CC, advantages and disadvantages of CC from participants based on their everyday experience and a discussion of themes from the interview based on the TOE framework are also discussed in this chapter. The research timeframe as well as ethical issues related to this research are also discussed in this chapter. The limitations are also discussed in this chapter. The final section of this chapter presents the results of this research.

3.1 Methodology

Methodology is regarded as a tool for conducting research. This includes the underlying philosophies, research approach, research strategy, choice, and time horizon. In order to provide an understanding of the methodology that will be employed in this research, Saunders, Lewis, & Thornhill, (2007)'s research onion will be used. It is important to note that methodological decisions are influenced by the epistemological, ontological, and axiological assumptions of the research. This chapter describes how the research was conducted. The research philosophy and approach, strategy, data collection and analysis techniques that were used in this research will be discussed in this section. The way the researcher plans to ensure that the chosen techniques and methodology will be appropriate in answering the research questions correctly without any bias will also be discussed in this section.

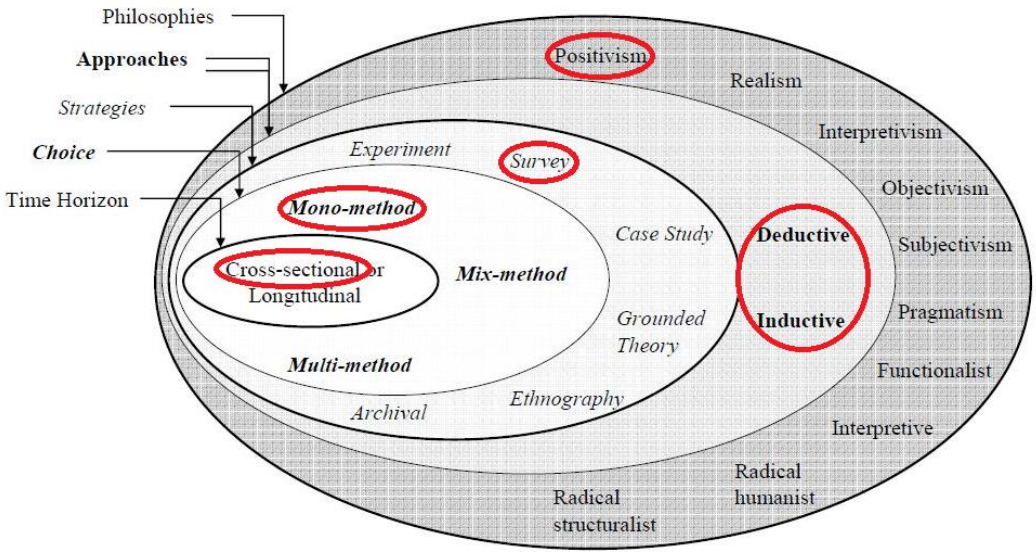

Figure 6: Research onion (Saunders, Lewis, & Thornhill, 2007)

The philosophy, approaches, strategy, choice, and time horizon in the red circles in figure 6 were used in this research.

3.2 Underlying philosophy

In order to design the right methodology and provide a clear understanding of the research approach, it is important to understand the underlying philosophy as it will assist in developing knowledge within the research area (Saunders, Lewis, & Thornhill, 2007). It is important to focus on the research philosophy from the beginning of a research because this will assist the researcher in determining whether the data collection method is appropriate to answer the research question (Saunders, Lewis, & Thornhill, 2007).

The epistemological, ontological, and axiological assumptions will now be discussed in details.

3.2.1 Epistemology

The main focus of epistemology is the field of knowledge with particular emphasis on acceptable knowledge in a field of study (Saunders, Lewis, & Thornhill, 2007). Epistemology refers to a general assumption about the right ways to investigate the nature of the world. It explains the process of knowledge creation and how the researcher's assumptions affect the created knowledge.

Epistemology has three main assumptions which are the positivist assumptions, interpretive assumptions, and critical assumptions. This research used positivist philosophy because it assumed that reality is objective and has measurable properties which are independent of the researcher's instruments (Myers, 2009). This allowed the researcher to be able to obtain original knowledge from the interview participants based on sense, experience and positive verification. This research also viewed knowledge as a set of data that is observable, measurable, and can yield a generalizable conclusion (Saunders, Lewis, & Thornhill, 2007).

3.2.2 Ontology

Ontology refers to the assumptions made by researchers about the nature of reality. It deals with the assumptions of the world and tries to establish the relationship between social entities and those assumptions. It is made up of objectivism and subjectivism.

Objectivism assumes that social entities are independent of social actors while subjectivism assumes that the perceptions and resulting actions of social actors produces social phenomena (Saunders, Lewis, & Thornhill, 2007). There is a tendency that the researcher might be bias when conducting a

subjective research because of his involvement with reality. Objective research however, has a lower chance of biasness on the part of the researcher because the researcher does not have a predetermined dependency between social actors and social entities.

3.2.3 Axiology

The main focus of axiology is on judgements related with values (Saunders, Lewis, & Thornhill, 2007). This explains why different researchers may arrive at different conclusions when they conduct the same research by highlighting how the outcome of the research is influenced by the researcher's judgement (Saunders, Lewis, & Thornhill, 2007). Axiology will not be discussed in details because the judgement of the researcher will not be used to determine the outcome of the research in this study. The outcome of this research was based on the outcome of the data gathering process. In order to clearly explain the processes that will be followed when conducting this research, the following section will discuss the research approach in details.

3.3 Research approach

The research approach is concerned with the processes followed when conducting the research. The two main approaches for conducting a research are inductive and deductive approaches.

The deductive approach uses empirical data collection to verify the validity of an already existing theory while the inductive approach aims at developing a theory based on observations and findings during focus group interviews or in-depth interviews with experts (Saunders, Lewis, & Thornhill, 2007). This research used a mix of both approaches because it verified the validity of the Technology, Organisation, and Environment (TOE) framework and also developed a framework based on the observations and findings during interviews with participants. The TOE framework was used in conjunction with the three steps for managing change by Kotter & Schlesinger, (2008) and the data obtained from participants during the interviews to develop the new framework called "Becoming Cloud Computing Ready" (BCCR). The BCCR framework aims to assist financial institutions to evaluate and improve their CC readiness

The researchers gathered empirical data from the literature review and the theoretical framework. The researchers also evaluated primary and secondary data and came up with a list of the barriers and enablers of CC readiness of SA financial institutions. The following section will discuss the research strategy.

3.4 Research strategy

It is important to select the right strategy as this includes the research outline, research tools, data collection techniques and research limitation. Research strategy includes archival research, action research, ethnography, grounded theory, case study, experiment, and survey (Myers, 2009; Saunders, Lewis, & Thornhill, 2007). The way data is collected and analysed differs from one strategy to another. All the research strategies are independent of each other and they could each be linked to descriptive, exploratory and explanatory research. Some of the strategies can be applied to both inductive and deductive approaches (Saunders, Lewis, & Thornhill, 2007). Archival research is concerned with making use of old documents that are sorted and organised for record purposes. Action research is concerned with providing solutions to real world problems and making substantial contribution to academic knowledge (Saunders, Lewis, & Thornhill, 2007). Ethnography requires field observation by the researcher in order to gain insight into what is happening in social environment. Grounded theory is concerned with development of a theory from the data that has been collected and analysed. The aim of case study is to explore existing real life situation when the difference between concepts are not clear. Experiment aims to verify, falsify, or establish the validity of a hypothesis using a trial and error procedure. Surveys are used to get data from selected participants and the data collection techniques used in surveys include questionnaire, structured observation and structured interviews (Saunders, Lewis, & Thornhill, 2007).

The most appropriate strategy for this research has been found to be surveys because the researcher aims to gather data from participants who will be selected based on their knowledge of CC and the positions in their respective organisations. An inductive approach will be used to conduct the survey so that the researcher can observe participants reaction towards the phenomenon and be able to draw conclusions. The research deign is guided by the research objective.

The data collected can be collected qualitatively or quantitatively or a mixture of both methods could be used. It is important to note that regardless of the difference between the two methods, they overlap with each other. It is also important to note that both methods are independent of each other and both have strengths and weaknesses. This research used qualitative method which provided the researcher with a better understanding of the people, the society and the environment they live (Myers, 2009). The key strength of qualitative research is that it obtains real life occurrences by focusing on naturally occurring events. Its key weakness is that results obtained are not always generalizable. Table 4 highlights the differences between the two research methods. This research

conducted semi structured interviews in a natural setting and obtained rich and deep data based on participants' point of view. The researcher was close to the participants as the interview were conducted face to face and the participants were able to provide answers in their own words.

Quantitative	Qualitative
Numbers	Words
Researcher's point of view	Participants' point of view
Researcher distant	Researcher close
Theory testing	Theory emergent
Structured	Unstructured
Generalization	Contextual understanding
Hard, reliable data	Rich, deep data
Macro	Micro
Artificial setting	Natural setting

Table 4: Quantitative and qualitative contrasts (Bryman & Bell, 2007, pg.426)

This research employed qualitative approach and only one strategy was used. It is therefore a mono-method (Saunders, Lewis, & Thornhill, 2007). Qualitative research provides a stronger foundation for the analysis and interpretation of data in the business environment because the setting is in the natural environment (Hussey & Hussey, 2003). The techniques used in qualitative analysis include interview, questionnaire, observation, and diary methods. The most commonly used methods for qualitative research is interviews and questionnaire which have been tried and tested extensively by several researchers (Bryman & Bell, 2007). There are three basic forms of interview. The first is open interview also known as unstructured interview in which the researcher engages in an informal conversation with the participant and the researcher is able to direct the interview. The second is pre-coded interview also known as structured interview in which researcher maintains total control of the interview and read from a prepared script. The third is a semi structured interview which is a combination of open and pre-coded interviews. In a semi-structured interview, the researcher has a list of the main issues to be discussed but the participant is allowed to raise any other issues that are relevant but not mentioned by the researcher.

In order to avoid biasness on the part of the researcher and allow the participant to contribute freely, semi-structured interview was employed for this research. Semi-structured interview will be discussed in the next section.

3.4.1 Semi-structured interview

Semi-structured interview allows participant to contribute a significant amount of data and discuss issues that the researcher might have ignored. It gives the participant freedom to speak about the topic from their point of view (Myers, 2009). Semi-structured interview will allow the researcher to address all the required questions and also pick up additional information. Interviews are like a night goggle which allows a researcher to see the things that are not ordinarily on view and to observe what is looked at but rarely seen (Myers, 2009). In order to ensure that the researcher does not miss any relevant information during the interview, the interviews were recorded and the researcher listened to the recordings to verify the information. The role of the researcher was to listen, encourage, record, prompt, and direct the interview process and allow the participants to use their own language rather than imposing his own (Myers, 2009).

3.5 Summary of research strategy

Table 5 is a summary of the research strategy employed by this research

Component	Approach & Short Description
Research Method	Qualitative. The objectives of this study have a perfect fit with results which can be produced by the researcher from qualitative research methods.
Philosophical and Epistemological Perspective	This research employed the use of positivist research because the methods applied in this study were based on the research questions being addressed.
Key Analytical and Descriptive Frameworks	TOE framework
Research Instrument	This research used open ended interviews. The duration of each interview was between one and two hours on average.
Participants	In total 12 participants were interviewed. Four participants are from the banking sector, four participants are from the insurance sector while the remaining four participants are from consulting companies that work for financial institutions
Mode of Analysis	Thematic analysis
Type of Study	Empirical and design because a framework was developed in this research
Unit of analysis	Financial institutions is SA (Banks and Insurance companies) and external consultants to financial institutions
Cross-sectional / Profile	Profile study. Interviews were carried out from March 2013 to October 2013

Table 5: Summary of research strategy

The following section will discuss the data collection process in details.

3.6 Data collection

3.6.1 Sample design and sampling methods

In order to conduct an extensive research that will cover a substantial part of the financial institutions in SA, participants were selected from both banking and insurance sectors. A decision was also made to identify consultants from external organisations that work with these financial institutions so as to allow triangulation and be able to validate the data collected from financial institutions.

The major banks and insurance companies in SA were identified based on their customer base, size, and number of employees. A letter was sent to all the identified organisations seeking their participation in the research. A list of participating organisations was compiled after response was received. Efficiency of research depends upon reliable and valid data collection. Chisnall, (1997) and Saunders, Thornhill, & Lewis, (2009) noted that the use of interviews can help to gather valid and reliable data that are relevant to the research questions and objectives. Data can be grouped into primary or secondary data (Chisnall, 1997). Primary data is data that has been collected for the first time while secondary data is the existing information that may be useful for the purpose of specific surveys (Chisnall, 1997). This research made use of both primary and secondary data. Primary data was collected through interviews and secondary data was collected from similar technology readiness studies. Interviews were arranged with the managers of relevant teams in the respective organisations for qualitative data. Because of the costs of travelling to all the organisations for the interviews and the possible difficulty in arranging meetings with respective stakeholders, telephonic interviews were conducted in some cases.

Once the sample was identified, letters were sent to different banks, insurance companies as well IT firms that work with these banks and insurance companies. Getting a response from these organisations proved difficult and time consuming and the researcher decided to arrange meetings with managements of the different organisations. After several attempts, approval was obtained from four major banks, four major financial institutions and four consulting firms that work with the banks and insurance companies.

Although the sample size was small and there were only four banks and four insurance companies represented in this research, it is important to note that the results of this research is generalizable for financial institutions in SA because the banks and four insurance companies that participated are

big firms that dominated their industries and owns majority of the market shares in financial industries in SA.

After the approval was obtained, participants were identified through enquiry from management and consent letters were sent out to participants. The participants from the banks and insurance companies were all members of their respective IT departments and are involved in the IT and CC decision making. The participants from the consulting firms are all working with these banks and insurance companies and providing them with advice on their CC implementations.

3.6.2 Data collection methods

After the participants were contacted and their consent was received, interview dates were set with each of the participants. The interviews were conducted from March 2013 to October 2013. This was because some participants had to cancel the appointments because of their organisational commitment and on those occasions, a new appointment had to be set. After several efforts, all the interviews were conducted successfully.

3.6.3 Data capturing and data editing

The interviews were all recorded and the recordings were transcribed into a text format by the researcher. Thematic analysis of the data was then conducted in order to identify, analyse, and report themes in a data. This was also very useful during transcription, data familiarisation, code generation, themes searching, defining and naming themes.

3.6.4 Design of the interview question

This research structured the interview questions based of the selected research framework in a way that suitable answers will be provided for the research questions. Because this research employed a qualitative method, the researcher needs to ensure credibility and transferability. Credibility is concerned with how trustworthy the research findings are and how the presented findings are accepted by others. Transferability is concerned with the possibility of applying the research strategy, approach, and findings to a similar study with the hope of getting similar results. See Appendix D for the research questions.

The interview questions were designed based on available literature on CC and TOE framework. Several themes were identified from literature and grouped based on TOE framework in order to provide answers to the research questions. In order to verify the validity of the questions, a pilot test was conducted in which three participants were interviewed. The first participant was from the

banking sector, the second participant was from the insurance sector while the third participant was a consultant that works with clients from financial institutions. After the pilot interviews, the researcher was able to identify limitations and weaknesses within the interview design and was able make necessary revisions before the implementation of the study. The pilot test assisted the researcher with the refinement of research questions. The research questionnaire consists of a brief introductory section, a section on participant's rights, a section on general questions and a section on CC. Refer to Appendix 9.4 for complete interview guide.

3.7 Data collection limitations and assumptions

One of the possible limitations of the data collection method is that it might be difficult to identify the most suitable participant in the organisation who will have all the necessary knowledge of CC required to answer the interview questions correctly. The cost of travelling to and from each participating organisation may be a limiting factor for the chosen data collection technique because the researcher will have to go to all the participating organisations for a face to face semi-structured interview with the selected participant.

3.8 Validity

Validity is concerned with ensuring that the findings reflect exactly what the research objective was. This will ensure that the research purpose and objective is fulfilled. Some researchers including Mason, (2002) have critiqued the validity of qualitative research. Mason, (2002) further went on to say that qualitative research lacks credibility, validity, and generalizability. This research is not in total agreement with Mason, (2002) because although generalizability is difficult with qualitative research, credibility and validity has been proven by several researcher when conducting qualitative research and they have been able to provide accurate answers to their research questions (Saunders, Lewis, & Thornhill, 2007).

Two type of validity have been identified to pose a threat to the credibility of a research. They are internal validity which is concerned with the interview participants. This can be because the participant does not have required knowledge about CC or s/he is biased because the outcome of the research may affect his/her job. In order to overcome these threats, the researcher will conduct a prior investigation by going to the participating organisations to identify suitable participants with the necessary knowledge of CC.

The second type of validity is the external validity which is concerned with the application of the research findings to similar situations. Once the data has been collected and the reliability and validity has been verified, the data needs to be analysed to derive meaningful information from the data. The following section will discuss the data analysis process in details.

3.8.1.1 Conference presentations and publications

In order to verify the relevance of this research and to further validate the data obtained during the data gathering process, part of this research was submitted to the 2013 IEEE International Conference on Electronics Technology and Industrial Development and was presented by the author at the conference on 23rd of October 2013 at the conference venue in Bali, Indonesia. This conference enabled the researcher to get valuable feedback from the participants and those feedbacks were then used to improve the research.

Another part of this research was later submitted to the 2013 IEEE International Conference on E-leadership hosted by University of Pretoria from November 4 to November 6, 2013. The submitted paper was accepted and also presented at the conference on the 4th of November 2013 and valuable feedback was also received from researchers from academic and industry and was considered to improve the output of the research.

After necessary improvements had been made to the research, a final section of this research was submitted and accepted for publication at the International Conference on Cloud Computing (ICCC) 2013 held in Wuhan China from December 1 to December 2, 2013. Relevant comments from this conference was also considered and applied to improve the final output of this research.

The conference papers which were part of this research and presented at the various international conferences in Indonesia, SA and China respectively gave the researcher an opportunity to interact with other researchers from different institutions and industries across the world. This has assisted the researcher in ensuring that the research is relevant and the contributions would be of great value to both academics and industry stakeholders.

3.8.1.2 Feedback from interview participants

In order to further validate the credibility of the data and framework in this research, the transcripts of the interviews was sent to the participants to ensure that the transcripts reflect exactly what the participants said. After the framework was developed, the researcher sent copies of the framework to all the interview participants in order to get valuable feedback which was later used to improve the framework. The feedback from the participants showed that the data and framework are relevant and would be a useful guide for financial institutions in the CC adoption.

Three of the participants said the framework gives a complete view of things to do in order to prepare for CC adoption. Seven other participants said that the framework covers all the CC issues and concerns that was identified in their organisations and would be a useful tool to improve their CC readiness. PI1 said it is a well thought framework and the addition of change management in the framework makes it more useful and would increase the chances of success with their CC adoption and implementation. Finally, PB2 said that the framework will serve as a guideline for their CC adoption as it covers all the important issues of CC. All the participants requested a copy of the final paper as they feel that the BCCR framework will help them towards improving the CC readiness.

3.9 Limitations

There were a number of limitations during the data gathering and analysis process. One of the limitations was that it was difficult to get hold of the participants. The original time planned for data gathering was four months but due to the difficulty in getting hold of some of the participants; it took over 7 months for the data gathering process to be completed. Another important factor for this research is the timeframe as this may have effect on the processes involved in this study. The following section will discuss the research timeframe in detail.

3.10 Research timeframe

A research time frame can be longitudinal or cross-sectional. Longitudinal time frame takes a longer period of time while cross-sectional time frame focuses on issues in a specific time period. Cross-sectional research timeframe provides a snapshot of the variables of interest for the research problem within a short time period. Because of its time constraint, longitudinal time frame is not suitable for this research as it is a research at master's level which has to be completed in a specific time period. Because the research was conducted in a specific time period, instrumentation, mortality and maturation did not constitute threats as they generally suffix in longitudinal studies

where the research is conducted over a longer time period and there might have been significant changes in the phenomenon being investigated (Saunders, Lewis, & Thornhill, 2007).

Ethics and confidentiality is also an important consideration to ensure that participants give accurate data during the data gathering process. The following section will discuss the ethics and confidentiality issues with this study.

3.11 Ethics and confidentiality

The interview questions were approved by University of Cape Town's (UCT's) ethics committee. Permission was requested from the selected organisations in order to gain access to their staffs for the interviews. There was an introduction section in the questionnaire which addressed ethical aspects of the study. There was also be a section asking respondents if they understood what the research was all about and the risks involved in participating in the questionnaire. The respondents were informed that their participation in the study was voluntary, and that their anonymity would be protected. The names of their organisations are also kept confidential and are not included in the report. The respondents were also informed that all the data obtained during the study will be treated as confidential. Respondents were also asked for email addresses that are not work related for follow up communication after the interview so as to ensure their confidentiality.

3.12 Summary of chapter

Participants were selected from banks and insurance in SA based on their size, number of customers and number of employees in order to obtain a sample that could be representative of financial institutions in SA. Participants were also selected from consulting firms that work for financial institutions and make most of their IT decisions for them. This was a very useful form of triangulation as it allowed the researcher to verify the data obtained from the banks and insurance companies from an external observer with good knowledge of the industry and CC.

Qualitative research approach was found to be the most appropriate for this research because of because of its ability to provide a strong foundation for the analysis and interpretation of data in the business environment. Semi structured interview was found to be the best qualitative technique as it allows participants to express themselves freely. This research adopted thematic analysis method because it has been found to be efficient in analysing textual and qualitative data. This was very

useful during the analysis stage as it assisted the researcher to identify, analyse, and report themes in a data.

The duration of each interview was between 1 to 2 hours. All the participants had knowledge of CC and are involved in making IT decision in their respective organisations. The number of employees in the participating organisations ranged from 500 + to 40000+. Each participant was able to give their own understanding of CC. They also identified some of the advantages and disadvantages of CC based on their everyday experience. Some of the important skills necessary for a successful CC adoption were also identified. The researcher was able to analyse all the issues discussed using the TOE framework.

Although, the sample size is small, it is important to note that the result of this research can be generalised across financial institutions in SA. This is because the sample size constitutes majority of the industry and own majority of the market shares due to their size, number of customer and number of employees.

The data analysis provided answers to the research questions by identifying the barriers and enablers of CC. The factors used to develop the proposed framework were also identified during the data analysis. The level of CC readiness of SA financial institutions was also found to be low and is still in the early stages as most of the financial institutions have not made provisions for all the readiness factors. They are still trying CC by using it for their non-core activities like managing their customers.

4. Data analysis

4.1 Mode of analysis

The data collected was analysed using qualitative data analysis (QDA) modes commonly used to analyse textual data. The large amount of data that a researcher always ends up with in an interview makes it necessary to analyse and interpret the data to edit and reduce the volume of data into smaller and meaningful data that explains the solution to the research question. Qualitative data analysis approaches will help to achieve that (Myers, 2009).

The modes of analysis available for analysing qualitative data are semiotics, narrative analysis, and hermeneutics and thematic analysis. This research adopted thematic analysis because it has been found to be efficient in analysing textual and qualitative data (Attride-Stirling, 2001). Thematic analysis is used to identify, analyse, and report themes in a data. This was very useful during transcription, data familiarisation, code generation, themes searching, defining and naming themes. This research also used inductive analysis method which helped to ensure patterns, themes, and categories of analysis were derived from the data gathered and were not as a result of pre-imposed suppositions prior to data collection and analysis.

Once the data gathering process was complete, the data analysis process began. The researcher analysed the data using thematic analysis by following the six steps of analysing qualitative data by Braun & Clarke, (2006).

The first step was familiarisation with data. During this step, the researcher transcribed the data and went through it several times to understand the data. After the researcher was familiar with the data and were confident that the data is consistent with the purpose of this research. The researcher then started generating codes by looking out for interesting features in the collected data and making notes of each feature.

The following step was to search for themes and extracting data relevant to the themes. After generating the themes, the researcher then performed a review of the themes in order to determine if the themes fit with the data. The themes were further reviewed, defined and named to refine specific of each theme. The final step was the production of the report. This was the process in which the researcher performed a final analysis by choosing valid and relevant extracts that related to literature and research questions in order to provide accurate answers to the research questions.

4.2 Overview of interview results

4.2.1 Interview duration

Each interview lasted for about one to two hours and the participants were allowed to respond to the questions in an open manner so as to prevent the researcher from influencing their response.

4.2.2 Profile of participants

All the participants from the banks and insurance companies were from IT while all the participants from the external organisations were consultants. The table below shows the participants role and years of experience. This research refers to participants from the banks as PB1, PB2, PB3, and PB4. The participants from the insurance companies are referred to as PI1, PI2, PI3 and PI4 while the participants from the consulting firms are referred to as C1, C2, C3, and C4 in order to ensure their confidentiality and that of their organisations. The years of experience of the participants are from 2 years to 15 years. All the participants have experience of CC and are involved with IT decision making in their organisations. This makes them suitable candidates for this research. Table 6 shows the profile of participants, their role in their organisations, years of experience and CC experience.

No	Participant	Years of experience	Role in organisation	Have cloud computing experience?
1	PB1	10	IT Manager	Yes
2	PB2	8	IT Infrastructure Product and Service Strategy	Yes
3	PB3	4	IT Architecture and Decision	Yes
4	PB4	7	IT Manager	Yes
5	PI1	6	IT Strategy	Yes
6	PI2	2	IT Infrastructure	Yes
7	PI3	5	National Manager: Networks and Telecommunications	Yes
8	PI4	9	IT Strategy	Yes
9	C1	15	Consultant and head of cloud computing centre	Yes
10	C2	4	Consultant	Yes
11	C3	9	Consultant	Yes
12	C4	11	Consultant	Yes

Table 6: Profile of participants

4.2.3 Number of employees

The banks, insurance companies and consulting companies where the participants work are all large organisations with several branches across SA. The number of employees range from 500+ to 40000+. The Banks are referred to as B1, B2, B3 and B4. The insurance companies are referred to as I1, I2, I3 and I4 while the consulting companies are referred to as CF1, CF2, CF3 and CF4 for confidentiality purposes.

4.2.4 Participants by role in IT decisions

All the participants from the banks and the insurance companies are involved in taking IT decisions for their organisations. The participants from the external organisations are consultants and are sometimes involved in taking IT decisions for their clients in the financial industry.

4.2.5 Participants understanding of cloud computing

In terms of their understanding of CC, all the participants have knowledge of CC and were able to give their own definitions of CC based on their experience. Some of the definitions of CC by the participants are:

"Using computing services on demand at a specific cost either based on utilisation or allocation of resources. Cloud can be private or public" (PB1)

"Cloud computing provides organisation with cheaper computing power over the internet. It is based on a pay as you go model where users only pay for the services they use" (PB2)

"I know that cloud computing refers to the provisioning of computing resources over the internet to people in different locations. Its aim is to save cost and it achieves that through its payment model where people can pay for only what they use" (PB3)

"Cloud computing generally refers to providing resources such as software and infrastructure to users over the internet and allowing them to pay per usage" (PB3)

"Cloud refers to the consumption of networked computing resources" (PI1)

"CC is the ability of an organisation to use infrastructure in the cloud or off premises and not having to worry about the capex outlay from a physical infrastructure point of view but rather buy this as a service from a cloud provider" (PI2).

"Cloud computing allows organisations to have access to infrastructures, software and platforms on a pay per use basis without having to purchase and own them" (C1)

"Technology solutions where critical infrastructure sits in the cloud. This includes email, applications, backups etc." (C2).

All the participants have good knowledge of CC and were able to describe CC from different views. Based on the various definitions, cost is of high importance to financial institutions because they

mostly refer to the ability of CC to reduce cost. C1 is the head of cloud computing centre in their organisation. C1 noted that CC adoption in SA has been currently slow when compared with countries in Europe or Unites States of America (USA). C1 also noted that in Africa, SA is more advanced in terms of CC adoption but is about 7 years behind in terms of adoption rate when compared with countries in Europe or USA.

Most participants also noted the ability of CC to allow users to pay per use. This is also an important factor for financial institutions because they believe it will help them reduce cost.

4.2.6 Advantages of cloud computing from participants

Some of the advantages of CC mentioned by the participants are:

1. Cost reduction and flexibility (C1, PB1, PI2, PI3, PI4 & PB4).
2. "Cloud allows you to focus on the things at add competitive value e.g. why build a CRM system when you can get it in the cloud? Rather deploy those resources on initiatives where you can gain competitive advantage" (PI1).
3. "Do not need expertise on the building of the components for a service you need. You just pay for it whilst expertise is held with the service provider" (PB1).
4. Ability to provide resilience (PI2).
5. Paying for a service and not investing in people and hardware to provide a service to your stakeholders (PI2).
6. Lower capital outlay, easy to update technology (C2).
7. Ability to work from anywhere (C2)
8. Faster time to market (PB4)
9. It allows quick deployment and
10. It provides easy access to resources. The service availability is also very good. For example "if we require 100 gigabytes of server space and tomorrow, we require 500 gigabytes which is five times our initial requirement, the service providers have that already and they will make it available to us immediately" (PB2).

The advantages of CC mentioned by the participants also show that cost is the most attractive to financial institutions. The flexibility of CC is another important factor for financial institutions. It is clear that the participants understands CC and knows how their organisations can benefit from CC. The researcher found it surprising that the participants did not mention the ability of CC to bring

growth and expand their customer base. This is possible because CC has the ability to connect all the branches of the banks including the ones in rural areas and provide them with facilities such as storage and computing power which would normally not be available in such areas.

4.2.7 Disadvantages of cloud computing from participants

Some of the disadvantages of CC mentioned by the participants are:

1. Security and the lack of full control of the environments that you know are yours (PI2). Security issue is a serious problem with CC.

2. Vendor lock-in. Another problem is the possibility of not being able to move from one service provider to another when you are no longer happy with you service provide (PB2). “There are many potential problems; the thing is not all vendors are made equal. You have to conduct a proper due diligence to ensure that you mitigate all the risks” (PI1).

3. Lack of detailed understanding of SLAs i.e. downtime and commitment mean time to recovery (MTTR) (PI2).

4. Business continuity. “When there is an outage, it will seriously affect our business as we need to be online every moment without any interruptions” (PB4).

5. Integration is also complicated with CC and it can be a daunting task to integrate your existing infrastructure with CC (PB4).

It is not surprising that security is of high concern to financial institutions. All the participants mentioned security as a very important factor to consider. The possibility of data lock was also found to be of serious concern for financial institutions. It is surprising that all the interview participants did not mention legislation and jurisdictional issues among the disadvantages of CC.

It was assumed before the interviews that because of the bandwidth issues in SA, CC’s dependence on the internet will be among the top disadvantages that would be mentioned by all the participants. The researcher found it surprising that only PB1 mentioned this disadvantage. The other participants did not mention CC’s dependence on internet as one of the top disadvantages of CC.

4.2.8 Data findings based on TOE framework

4.2.8.1 Technology

4.2.8.1.1 Security

Most of the participants mentioned security as the most important factor to consider when adopting CC especially for financial institutions that deal with sensitive data and confidential information of clients. “Security is paramount but there are many other things to consider depending on the use case” (PI1). PB4 also noted that security is the most important factor. He also mentioned that they have not considered implementing CC on a full scale because of the security issues.

PB1, however has a different opinion and disagrees with the fact that security is the most important factor. Although he agrees that security is an important factor, he noted that cost and quality of internet services are important to keep a consistent experience is the most important factor to consider in ensuring uninterrupted services especially when up to date information is needed to conduct business activities. An example he gave was the need for constant connection in the foreign exchange department where current and up to date information is needed to determine the exchange rates. Other important factors to consider are speed and performance (C2).

In order to ensure proper security in the cloud, insurance 1 conducts thorough due diligence for each engagement. The data classification of the solution drives the set of controls that they deploy.

I2 have security measures in place and PI2 mentioned proxies set up and intrusion protection systems (IPS) as some of the security measures they have in place.

B1 on the other hand does not have security measures in place as they rely on the cloud provider for these. PB1 however noted that they are currently looking at policies in order to come up with adequate security measures. B1 does not have processes for ensuring security and compliance for CC but all the other organisations have appropriate processes for ensuring security and compliance for CC.

C1 noted that as a general requirement adequate governance and risk governance need to be in place but from her observation, they are not in place in most of the financial institutions.

Data management as well as identity and access management are also important security measures to make sure that only valid persons have access to information (C1).

In terms of access and adding users who need to access cloud based services, all the participating organisations rely on the cloud provider. This is risky because if the service provider has interest in their information, they can add a user who is not part of the client organisation in order to have access to the information that they need.

In general, cost and security came up several times for different questions. This shows that cost and security are the two most important factors for financial institutions. This correlates with literature as several literature also mentioned cost and security among the top issues with CC.

4.2.8.1.2 Cloud computing architecture

The architecture of CC in I1 is limited to IaaS (PI1). B1 and I1 are in the early development stages of their CC architecture (PB1 & PI1). C2 noted that some of their clients in the financial industry have their data stored in a local data centre with fail over and virtual environments that assist in minimising downtime.

Most of the participating organisations are re-architecting their applications to integrate it with CC while I1, I2, I3 have not done it yet but have plans to do it.

4.2.8.1.3 Governance

Most of the participating organisations have CC governance in place. PI1 noted that they have a mature governance process for all software acquisition and SLA management. PB1 noted that they do not currently have CC governance in place while PI2 noted that they are in the process of putting their CC governance in place. The participants all agreed that having CC governance in place is one of the most important steps towards a high level of CC readiness.

4.2.8.1.4 Quality of internet service

The quality of internet service is very important for CC to function effectively because cloud services are offered over the internet. CC service will only be as good the internet service because of its reliance on internet (Chauhan, Bansal, & Alappanavar, 2012). “It is true that security is of high importance, the cost and quality of internet service are equally important in order to ensure that cloud services are available continuously without any interruption” (PB1).

4.2.8.2 Organisation

4.2.8.2.1 Impact and business value of cloud computing

Organisations need to understand the change that CC will have on their organisation. From a business driver or strategy perspective, they need to understand the driver and they need to understand the implication on the organisation. Say for instance they use public cloud it will lead to a change in their business processes. It will affect the structure of the IT department and the nature of the operations would change so they need to understand the change it will bring to their business. "So for me, they need to understand readiness for cloud adoption i.e. they need to understand why they are doing it. They also need to understand what are the key risks? For instance, we don't have adequate bandwidth in SA or we are struggling with availability of power or whatever key risks. So you need to understand the drivers and the key challenges you need to overcome before you can actually do it. So you need to do some analysis of risks versus rewards" (C1).

In terms of the business value of CC, all the participating organisations have defined and measured the business value of CC except for I2. It is essential for I2 to also define and measure the business value of CC so that they can be able to determine the impact of CC on their business.

4.2.8.2.2 Skills and Training

In terms of skills, all the participants mentioned that proper understanding of CC is important as the organisations needs to know how CC will fit into their business and what impact it will have on their business. PB1 noted that understanding the implications of cloud services such as the need to be online for public cloud services is vital. General understanding of CC in terms of what would actually force the organisation to start using the technology is important. Things like mobility, things like workforce having access to information anytime, anywhere (C1).

It is also important to understand security requirements, project management, financial management, SLA and vendor management (PI2). "You need communication skills to be able to negotiate SLAs with service providers and also to communicate information to you employees. You also need to have some basic IT skills like using the internet as CC is provided over the internet" (PB2). Another valuable skill is teamwork and collaboration which are important for CC. An organization should encourage teamwork and collaboration as it will boost their understanding and cooperation to make the project work" (PB3).

From a cloud perspective it is important to understand the current architecture of your organisation and how that would integrate with your cloud solution (C1). This is dependent on the type of cloud your organisation is trying to adopt. For example, if it's private cloud, then the skill is similar to traditional IT. You need to set up a data centre and be able to manage it. They would definitely need to understand what CC really means. "If you start looking at public cloud, what it essentially means is that they need to have some integration skills. The cloud based solutions need to talk to your traditional on premises solutions and they need to understand the integration and the data flow. With public cloud, you also need to understand how to manage your service provider" (C1). Organisations need to find a way to manage their relationship with service providers and ensure that the service provider is delivering on what they promised (C1, C3, C4, PB2, PB3, PI1, PI3 & PI4).

In terms of CC experience, all the participating companies have employees with CC experience. PB1 noted that they are planning to send out technical experts to Amazon Cloud training.

C1 noted that they have a lot of capabilities, methodologies, frameworks where they assist clients to understand cloud readiness, cloud adoption, governance and risk management, change management and people management.

C1 was unable to ascertain whether or not financial institutions have that in-house but said generally, financial institutions would get them in to assist and help with their journey towards cloud adoption.

In order to ensure that employees are utilising CC to achieve all the expected benefits, training is essential so as to make sure that they know what to do whenever they need to make use of any cloud service. I1 and B1 do not currently have any training programmes on CC for their employees. I2 utilises training programmes on CC that are offered by their training partners. All the remaining participants noted that their organisations outsource this to organisations that specialise in CC training.

4.2.8.2.3 Attractive features of cloud computing

The ability of CC to help reduce cost of buying and maintaining infrastructure, software and applications attracts all the participating organisations. The value that CC adds to the business processes is also a source of attraction (PI1). Scalability and speed of deployment of needed infrastructure is another reason why CC is attractive.

Reliability and failover is another reason why CC is attractive to organisations because most cloud services have business continuity and disaster recovery plans which are critical for every organisation (C2). From a costing perspective, the capability of CC to reduce cost and change operational model of the organisation makes it attractive to organisations. Other reasons why CC is attractive to organisations are:

1. Being more agile. You have availability to resources on the go or on demand.
2. Cloud availability i.e. service providers have more space available and you can buy more when you need it.
3. Flexibility i.e. you only buy what you need and
4. It gives organisations the ability to be more innovative (C1)

4.2.8.2.4 Cloud computing services used

Most of the participants noted that cloud is being used, and the usage is increasing. Cloud usage is limited due to strong security and regulatory requirements the bank adheres to (C1 & PB1).

B1 uses Customer Relationship Management (CRM) services, Dropbox, Google and Apple Cloud services. I1 uses SaaS and PaaS offerings are currently building a private cloud for IaaS (PI1). I2 is currently not using any cloud service but is considering using them in future.

B2 uses Condeco which is an office, facility space, and service management software for things like office space management, data management for example, to generate reports and these are hosted in the cloud. “Our CRM is also cloud based” (PB2).

B3 uses cloud CRM and they also use Tivoli Provisioning Manager (TPM) from IBM which is a storage management and data protection application on the cloud. “We also use the amazon web services (AWS) which allows millions of our mobile banking customers to be able to access our systems and perform transactions at the same time without any overload issues. We also use AWS for marketing and customer support” (PB3).

B4 is still in the early stages of the CC implementation. “We only use cloud for less sensitive operations but we are looking forward to using more of CC especially once there is a solution about the security issues” (PB4).

All the participants from the banks and insurance companies noted that they are currently using cloud for their non-core processes and the cloud services they currently use include email, backups, collaboration based applications and applications to manage their HR processes or CRM while the consultants also confirmed that.

4.2.8.2.5 Management

I1 has several management capabilities to ensure that their CC adoption is successful. They currently have two SaaS vendors that they manage and their infrastructure teams are tasked with managing the vendors because their infrastructure management is outsourced.

B1 and I2 currently have no management capabilities in place and they rely on SLA to ensure that the cloud provider deliver what was promised. C1, C3 and C4 confirmed this as they noted that few of the financial institutions have management capabilities in house as majority of their clients in the financial industry either rely solely on the cloud provider for these or outsource it to the consultants' organisation to manage their cloud infrastructure for them.

4.2.8.2.6 Business continuity and disaster recovery

Cloud provides disaster recovery in itself because the location of data is always different and as a result some of the participating organisations like I1, I3 and I4 are less concerned about BCDR. The banks have a different view on this issue when compared to the insurance companies view because all the participating banks have BCDR plans in place even though they are aware that cloud does provide BCDR in itself.

4.2.8.2.7 Strategy

All the participating banks have CC strategies in place while three of the participating insurance companies also have CC strategies in place. I2 is the only organisation that does not currently have a CC strategy in place but are looking to have one in place in future.

4.2.8.2.8 Communication

Communicating the results of CC initiative is important in order to allow employees to realise the benefits and impact of CC on their business. This would encourage them and help to reduce resistance from employees towards CC adoption. It was found that all the participating organisations except for B1 do not communicate the results of their CC initiative across their organisation. PB1 also

noted that although result of their CC initiative is always communicated, it is minimal with the business but widely communicated to the IT infrastructure community.

There is a need for improved communication of the results of CC initiatives to the entire organisation in order to reduce resistance and increase employee acceptance of CC.

4.2.8.3 Environment

4.2.8.3.1 Cost

The cost of CC is driven by environmental factors such as availability of bandwidth, competition among cloud service providers etc. Cost is not the most important issue as cloud is certainly not always cheaper. “You have to look at the entire business case to see what makes sense. Cloud is about additional value, that value is definitely more than just lowering cost” (PI1).

The costs of public cloud services are reasonable but quality of internet connectivity in SA does prohibit wide scale adoption of cloud services because of the bandwidth issues (PB1).

PB2 noted that cost is very important as their goal is to spend less where possible and still deliver the same or better quality of work. For B3, cost reduction is also an ultimate goal (PB2). “I think the cost in SA may be higher than the western countries because they are more advanced in terms of cloud computing and they have more cloud service providers which creates some kind of completion thereby forcing them to reduce their prices” (PB3).

C1 noted that in determining cost, several factors need to be considered i.e. are you using a public cloud or private cloud, are you talking of the capex costing or the apex costing? And it depends on availability of infrastructure i.e. whether or not you have adequate bandwidth. The type of application, the type of service, the type of network, availability and deployment model etc. are factor that determine the cost of CC.

The number of service providers available also determines the cost of CC services. For example, CC services are cheaper in USA because there are so many service providers and there is competition among the service providers in order to attract customers. This has contributed to reduction in the cost of CC services in USA. The cost of CC services in SA is there for more than in USA because of the availability of bandwidth and more service providers.

All the participating financial institutions have evaluated the costs and benefits of CC. The common thing among all the organisations in this regard is that they all outsourced the evaluation to external consulting companies. This is as a result of lack of evaluation framework or strategies in-house. This is surprising as it was expected that evaluation of CC would be done in-house in order to allow internal staffs who work with existing systems to determine whether there is need for CC and how it will fit with existing systems. When asked whether financial institutions evaluate the costs and benefits of CC, One of the consultants confirmed by saying "we do that for our clients so most financial institutions evaluated the costs and benefits of cloud computing before adopting it" (C1).

4.2.8.3.2 Regulations

Protection of Personal Information (POPI) Bill which was signed into law in November 2013 will help shape CC in SA. The POPI act will give effect to the right to privacy, by introducing measures to ensure that the personal information of an individual is safeguarded when it is processed by responsible parties who are in possession of such information (HumanIPO, 2013). What it basically means is that the location where the cloud provider stores data need to have a similar privacy law in place or the cloud provider will have to comply with POPI Bill.

In SA, we also have Electronics Communications Act (ECA) which regulates electronic communication. Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) and Financial Intelligence Centre Act (FICA) which are important for financial institutions are also available in SA. They are aimed at fighting financial crimes such as money laundering, tax evasion, and terrorist financing activities are also in place in SA and they will play a role in shaping CC in SA although their effect on CC will be minimal when compared with POPI and ECA (C1).

Sections 19 to 22 of the POPI Bill recommend security safeguards that service providers and client organisations need to adhere to while processing personal information (Kafouris & Houston, 2014). Responsibilities such as identifying risks to personal information; establishing and maintaining appropriate safeguards; verifying the effectiveness of safeguards; and updating safeguards in response to new risks or identified deficiencies were recommended in section 19(2) in order to safeguard personal information (Kafouris & Houston, 2014). Section 21 of the POPI Bill specifies that if an organisation requires a service provider to process personal information, a written agreement that stipulates that the service provider must establish and maintain safeguards to protect the integrity and confidentiality of personal information should be made (Kafouris & Houston, 2014).

In addition, chapter 9 of the POPI Bill deals with information flow across countries. It stipulates that an organisation may not transfer personal information to a service provider in a foreign country unless the service provider is subject to a binding agreement that ensures the requirements of safeguarding personal information; or the service providers are adhering to adequate laws in their country that similar to provisions in the POPI Bill (Kafouris & Houston, 2014). ECA stipulates that organisations have legal responsibilities with regards to the retention, destruction and restoration of stored information. This will includes information stored in-house or in the cloud (Viljoen, Solms, & Lawack-Davids, 2012). FICA and RICA stipulates that organisations keep information of their clients update them regularly. This will ensure that service providers keep proper records of their clients and are able to provide such information to law enforcement officers in case there is an irregularity such as money laundering or any other criminal activity in the cloud (C1).

4.2.8.3.3 Cloud providers

Cloud providers play an important role in the success of CC implementation. Choosing the right cloud provider is an important step for financial institutions in order to ensure successful adoption of CC.

To select the right cloud provider the first thing is to understand the current maturity, the current state of the IT landscape, the infrastructure, the architecture and how they interact with each other. Once the requirements are available, you can then come up with a list of cloud providers that offer those requirements which you have identified in order to choose from them (C1).

PI2 noted that functionality, ease of deployment, ease of upgrade, SLA and costs should be considered when choosing a cloud provider. C2 also noted that costs, reliability, security and ease of growth and changes should be considered when choosing a cloud provider and this is in agreement with PI2.

It is also important to verify the trustworthiness of a cloud provider before trusting them with your data. Some of the indicators that a cloud provider is trustworthy are track record in the market, number of clients in our industry or vertical, recommendations by research organisations, transparency shown during the due diligence, access to audit reports conducted by a third party and ability to provide evidence of controls and procedures (PI1). The reputation of the cloud provider is also important to determine their trustworthiness (PB1).

Another factor to consider is the responsiveness and pro-active thinking of the cloud provider. The level of innovation and ability to provide solutions even when these might not seem to suit them from a business point of view is another important factor to consider (PI2).

4.2.8.3.4 Government support

In terms of government support, all of the participants noted that there is no government support for organisations that are implementing CC in SA. C1 mentioned that with organisations overseas, although there is no specific government support relating to CC, government usually have broadband plans in place which enables organisations to use public cloud services. For example, in Kenya, the government conducted a research on how they can actually provide cloud services to the people in Kenya.

4.3 Readiness

In terms of readiness, organisations should understand why they want to adopt CC. Organisations need to know what values they want to derive from CC. They also need to understand the risks and the challenges involved with CC. Furthermore, they need to understand the impact of CC on the organisation versus the suitability. For example, if the impact is low and its highly suitable for the organisation then the organisation is more ready than if the impact is high and suitability is low (C1).

Some of the comments from participants about readiness are:

"Readiness is very important because if we are not ready, we would be wasting our time with cloud computing. Readiness means that we have identified what systems and data are best suited to the cloud. It also means that we have assessed the costs and benefits of cloud computing for our organisation and realised that it will bring us more benefits at a lower cost. We have not really analysed our systems to determine which ones are best suited for cloud computing so I think we are not yet ready for cloud computing" (PB4)

"For me, readiness would mean that we have adequate network capabilities and other resources like cloud computing skills and good internet availability" (PB3)

"In order for us to be ready for cloud computing, we need to ensure that we have enough funds and staffs with knowledge of cloud computing. We also need to have a good understanding of cloud computing and related technologies. This will enable us to know exactly how cloud computing will fit with our existing systems" (PI1)

"Readiness would mean that we have developed policies for assessing risk and managing governance. It would also mean that we have found a way to reduce all the possible risks of cloud computing" (PB2)

"Knowing what we need to take to the cloud and what we need to keep in-house on our existing systems is a good indication of readiness" (PI4)

"The first thing that tells me we are ready for cloud computing would be our understanding of our current systems and how they can be integrated with cloud computing" (PB1)

"I don't think financial institutions in SA are at the necessary level of readiness. There are still issues with poor bandwidth and security. Most financial institutions in SA also don't have strategies in place for cloud computing" (C3)

"I don't think we are ready for cloud computing. Having a good strategy in place is the first step towards readiness. Training facilities and availability of staffs with good knowledge of cloud computing is also important step towards readiness. We still need to work on that" (PI3)

"For me to acknowledge that we are ready, I expect to see it in our staff's willingness to accept change. This is because no matter what preparations we make, if our staffs are not ready for the change that cloud would bring, it simply means that we are not ready. At the moment, staffs have mixed feelings about cloud computing because some of them feel they might lose their jobs because of cloud computing. All of that needs to resolved before I can say we are ready for cloud computing" (PI2)

"I cannot say they are ready for cloud computing because they still have to develop strategies for cloud computing. Most financial institutions in SA still don't have strategies in place. They also don't have training programmes on cloud computing" (C2)

"Financial institutions in SA are on different levels of readiness. Some are more ready than others but generally, I think the readiness level is low" (C4)

Based on participant's comments, readiness could be measured in terms of resources available for CC. The ability of an organisation to identify what should be moved to the cloud and what should remain in the traditional system also shows readiness. Availability of funds to provide all the necessary resources for CC is another indication of readiness. Ease of integration of CC with existing

systems is another indication of readiness. Furthermore, having proper change management strategy in place is an indication of readiness.

In general, financial institutions in SA have a low readiness level in terms of CC adoption. This will improve in future as many of the financial institutions are taking steps towards increasing their readiness level.

5. The proposed framework: BCCR

This chapter presents the proposed framework called "Becoming Cloud Computing Ready" (BCCR). The framework was developed from a combination of the TOE framework, the change management framework and the data obtained during the interview. The framework is aimed at assisting financial institutions in SA to determine their level of CC readiness and help them improve their CC readiness level which will in turn improve their CC adoption success.

The first step towards readiness assessment is that organisations should understand why they want to adopt CC. They should ask themselves questions like:

1. What values do we want to derive from cloud computing?
2. What are the risks and challenges
3. They need to understand the impact on the organisation versus the suitability. For example, if it's low impact and it's highly suitable for the organisations then they are more ready than if its high impact and low suitability.

If the impact of CC on the organisation is low and the suitability is high the organisation can go ahead with their implementation. If the impact on the organisation is high and the suitability is low, the organisation does not need to implement CC at that stage.

Once the decision has been made on the impact and suitability of CC, if the decision is that CC will have a low impact and high suitability for the organisation, the organisation can then proceed with their CC readiness assessment. The BCCR framework can then be applied to determine the organisations readiness and improve it if necessary. Figure 7 shows the BCCR framework and the relationship among all the factors that affects CC readiness.

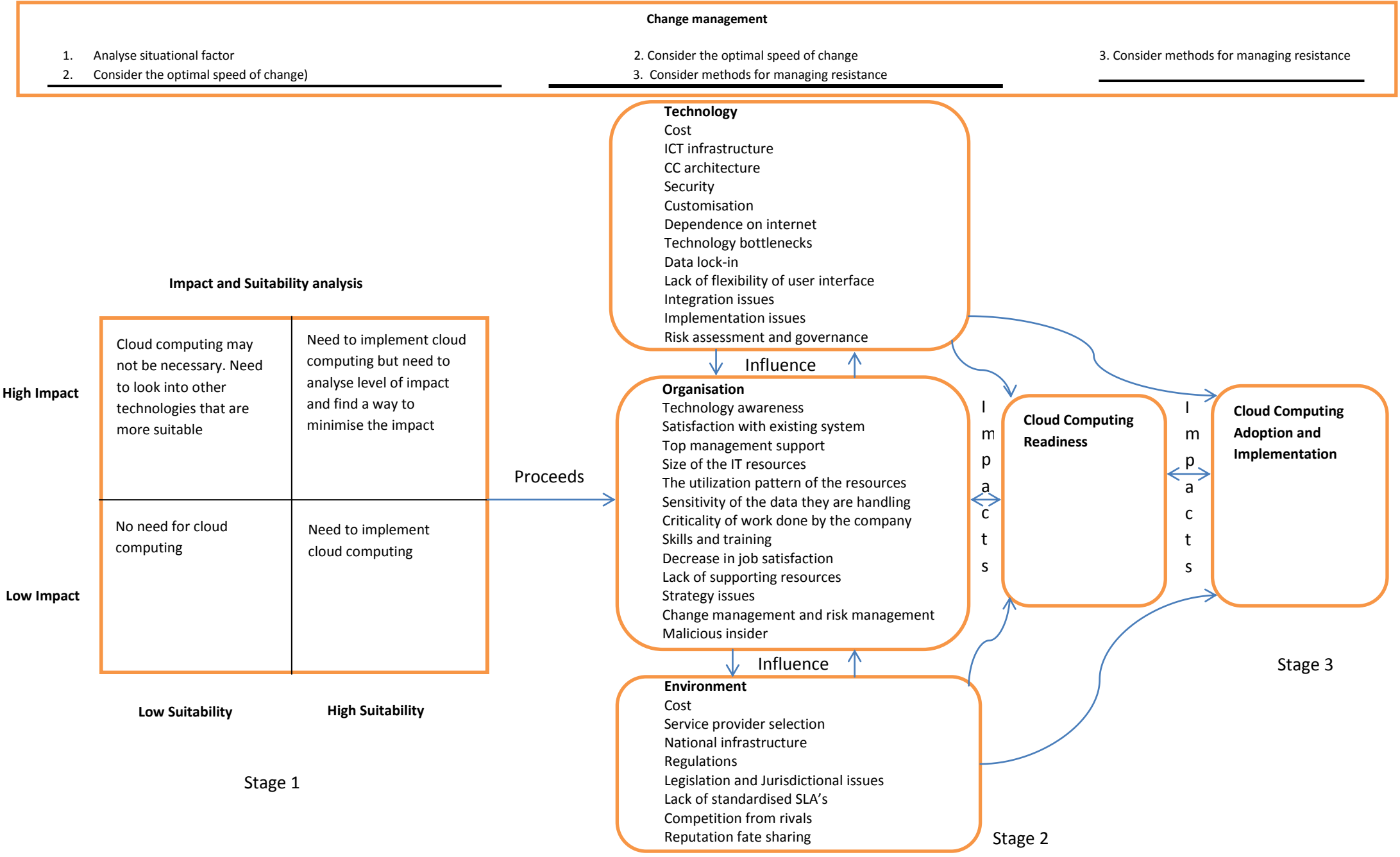

Figure 7: BCCR Framework for assessing cloud readiness

Figure 7 shows that technology and environment have a direct impact on the organisation and would affect the organisational CC readiness. It also shows that the organisational factors have a direct impact on CC readiness and the CC readiness of organisations also have a direct impact on their CC adoption and implementation success.

Figure 7 also shows that change management should be applied at every stage of CC implementation right from the readiness assessment stage through to the adoption and implementation stage. The three steps for managing change successfully by Kotter & Schlesinger, (2008) described in chapter 2 should be applied in all the stages as it will help to persuade and motivate people to help implement change. It will also make people feel more committed to making the change happen thereby increasing the CC readiness level of the organisation and increase the success of adoption.

Steps 1 and 2 of Kotter & Schlesinger, (2008)'s three steps for managing change successfully should be applied during stage 1 (impact and suitability analysis stage) of BCCR framework. The manager or change agent should identify the expected type of resistance and determine his relationship with people who are expected to resist change. The manager or change agent should also determine whether the change is urgent or not. The manager or change agent also needs to determine whether the change will be intensive or not. This will determine whether the change should be carried out slowly or quickly. This forms part of the step to determine the impact and suitability of CC on the organisation. As shown in figure 7, if the assessment shows that CC will have high impact and low suitability on the organisation, this means that CC may not be the right technology the organisation needs at that stage. The organisation should rather look into other technologies that are more suitable. If the assessment shows that CC will have a low impact and low suitability, it also shows that the organisation does not need CC at this stage. If the assessment shows that the CC will have high impact and high suitability, it shows that the organisation may implement CC but need to analyse the level of impact and find ways to reduce the impact as high impact may mean a complete change in their business process which may turn out to be very expensive for the organisation. If the assessment shows that CC will have a low impact and high suitability. This shows that it is the right time for the organisation to implement CC. The organisation can now proceed to do an assessment of technology, organisation and environment.

In stage 2 of BCCR framework, the manager or change agent should apply steps 2 and 3 of Kotter & Schlesinger, (2008)'s three steps for managing change successfully. The optimal speed of change

should be determined and methods for managing change should be considered. If there needed resources are available and there is top management support, this could mean that the change can be carried out quickly. If staffs are satisfied with the existing system, they should be allowed to participate in designing and implementing the change as this will let them see the reasons for change and increase their commitment to change. Finally, participation, facilitation, negotiation and coercion should be applied if there is a decrease in job satisfaction. Participation will assist in reducing resistance to change by staffs that might be affected by the change. Facilitation will provide emotional support and training for staffs and provide them with skills that will help the cope with change. This will help increase job satisfaction. Negotiation will also help increase job satisfaction because staffs will be motivated if incentives are offered during negotiation. Coercion can be applied if other methods prove ineffective. Staffs that are still not satisfied could be threatened with possible loss of jobs or promotion opportunities.

The arrow that links stage 1 and stage 2 of BCCR framework indicates that CC would have low impact and high suitability for the organisation and the organisation can proceed to stage 2. The arrows that link the technological, organisational and environmental factors show that the factors influence one another. The arrows that link stage 2 and 3 shows that the technological, organisational and environmental factors impact CC readiness and vice versa.

In step 2 of BCCR framework, for organisations with low readiness level, negotiation method in step 3 of Kotter & Schlesinger, (2008)'s three steps for managing change successfully should be adopted because it will allow the organisation to motivate everyone that would be needed to make CC adoption a success. Once a high level of readiness is achieved, CC can then be adopted. The different methods for managing change in step 3 of Kotter & Schlesinger, (2008)'s three steps for managing change successfully which are education, participation, facilitation, negotiation and coercion should be applied to every change encountered during CC adoption and implementation stage of the BCCR framework. This will ensure that everyone involved with CC adoption in the organisation has all the necessary education and are able to participate and make informed decision towards a successful CC adoption.

5.1 Technology

The technological factors include cost, ICT infrastructure, cc architecture, security, SLA, customisation, dependence on internet, technology bottlenecks, data lock-in, lack of flexibility of user interface, integration issues, implementation issues, risk assessment and governance. They should first be considered in order to check the organisation's capabilities in terms of the technological requirements of CC.

The cost of CC is the first factor that needs to be considered as it will be a waste of time to continue analysis if the organisation cannot afford CC. The organisation needs to make provisions for all the necessary infrastructure and architecture that will ensure there is continuous service availability in the cloud and the service, data, and infrastructure are available to authorised users immediately upon request (Armbrust, et al., 2009; Zissis & Lekkas, 2012). The organisation also needs to make plans to configure strong access control and API infrastructures that will improve security, integrity and data confidentiality. This will ensure that confidential and sensitive organisational data are not lost or exposed to unauthorised third parties once in the cloud.

The organisation should also determine if there would be any need for customisation of any of their applications of software in the cloud to meet their specific business requirements. This will help them in choosing a service provider that offers such level of customisation. Since CC relies on the internet for its services, the quality of internet service in a vital requirement for CC as poor quality of internet service will result in poor quality of CC services. The organisation needs to investigate the kind of internet services available to them and determine whether the quality of the available internet service meets the requirements of their CC service. All other known issues related to technology should be considered at this stage and proper plans should be put in place to provide solutions to them.

It is important to note that CC is still evolving and more issues may arise with time. Once those issues arise and they are identified, they should be included and proper solutions should also be put in place for them to ensure that the organisation is ready for CC adoption in terms of technology.

The issue of data lock-in should be considered as it will give the organisation the chance to negotiate with service provider from an early stage. This will also help resolve integration issues. Another important factor is lack of flexibility of user interface. The organisation should include this in the criteria to select service provider. Implementation issues should also be dealt with so as to find ways

to resolve them if and when they arise. Risk assessment and governance are also important because organisation's need to understand the perceived risks involved with CC and how to mitigate them.

5.2 Organisation

Organisational factors such as technology awareness, satisfaction with existing system, top management support, size of the IT resources, the utilization pattern of the resources, sensitivity of the data they are handling, criticality of work done by the company, skills, training, decrease in job satisfaction, lack of supporting resources, strategy issues, change management, reputation fate sharing, malicious insider and risk management should be considered at this stage.

The organisation needs to know about CC and related technologies so as to determine how it will fit into their business processes. The organisation also needs to look at the existing system in terms of cost, ease of use, efficiency and effectiveness and compare this with CC to determine if CC offers more benefit than the existing system. The support of the top management is another important organisational factor as most organisations fail in their technology adoptions because there is no support from the top management. The size of the IT resources is also important at this stage because it will assist in selecting the right type of cloud. If the organisation is a small organisation, it may be cost effective to go for a public cloud as the data centre and all other infrastructure will be provided by the service provider. If the organisation is a large organisation with large data centre, choosing a private cloud may be the best option for them because they already have their data centre and this will also give them control over their cloud infrastructure and ensure that security and privacy is improved. The utilisation pattern of resources is also important because organisations that utilise a large amount of resources should be able to use that to negotiate for lower price with the service provider. This will assist them in cutting cost in the long run.

The sensitivity of data is also an important consideration at this stage. This will assist the organisation to identify the more sensitive data and separate them from the less sensitive data. They will then be able to determine which ones to move into the cloud and which ones should remain in-house. The less sensitive data can be moved first into the cloud in order to test the cloud to see if it meets the organisational requirements. This will reduce the risks of data loss and other risks associated with moving into the cloud. The criticality of work done by the company should be considered at this stage because stringent SLAs, resources, platforms, applications and security are needed for highly critical works while requirements of less critical works may be flexible.

Another important consideration at this stage is skills. There are some skills important for successful adoption of CC. The organisations should arrange training for their IT staffs in order to equip them with the necessary skills. This will ensure that the staffs are able to tackle any issues that arise in a professional manner and avoid any problems that could have occurred as a result of lack of necessary skills. The possible impact of CC adoption on employees' job satisfaction should also be considered. It should be identified and necessary plans should be put in place to reduce such impact and improve employees job satisfaction as the success of adoption will be affected if employees' are not satisfied with their jobs as a result of changes from CC adoption.

Resources needed to support CC should be made available as this will ensure that CC runs smoothly. The organisation also needs to develop CC strategies that will guide them during and after implementation. Another important factor the organisation needs to consider is change management as CC will bring about change in their business. Risk management strategy should also be developed in order to reduce the risks identified. The possibility of having a malicious insider should also be considered and appropriate plans should be made to reduce possible risks as a result of malicious insider.

5.3 Environment

The environmental issues include cost, service provider, government support in terms of national infrastructure, regulations, legislation and jurisdictional issues, lack of standardised SLA's, competition from rivals and reputation fate sharing should be considered at this stage.

The cost of CC depends on environmental factors such as availability of service providers and availability of national infrastructure. The organisation needs to investigate these factors at this stage to determine their impact on cost as they may drive cost high if their availability is low in the environment in which the organisation is located. For example, if the availability of bandwidth is low, it will lead to an increase in the cost of CC. If service providers are also few in the environment, competition will be reduced and cost of CC will also be high. The organisation needs to find out about the available government support such as the available national infrastructure, available bandwidth and strategies that could influence CC. As noted by consultant 1, the government support for CC in SA is inadequate and this will in one way or the other affect the CC readiness of organisations in SA.

The organisation also need to carefully select a service provider by looking at the reputation of the service provider, the types of cloud services offered, functionality, ease of deployment, ease of

upgrade and changes, SLA, costs, reliability and security. It is also necessary to verify the trustworthiness of a cloud provider by looking at the track record of the cloud provider in the market, number of clients in the financial industry or vertical, recommendations by research organisations, transparency shown during the due diligence, access to audit reports conducted by a third party and ability to provide evidence of controls and procedures. The ease of moving to another cloud provider and the ease of integration with in-house application and infrastructures should also be considered. Another factor to investigate is the responsiveness and pro-active thinking of the cloud provider. Once all of these factors are considered, this will guide the organisation and assist them in choosing the right service provider and increase their chances of successfully adopting CC.

Regulations, legislations and jurisdictional issues should be considered at this stage because they will have an impact on the success of CC adoption. If there are regulations, legislations or jurisdictional issues that can help regulate CC, organisations should be aware of them and develop strategies in order to make sure that they meet the requirements of those legislations and regulations. Jurisdictional issues should also be thoroughly investigated as it will affect the success of their CC adoption. For example, the cloud provider may have their data centre in another location with different laws, regulations and legislations. The organisations need to know which law will be applied in this case and how that laws will affect them in terms of who owns the data, which laws, regulations and legislations are applicable etc. In SA, laws such as POPI, ECA, PIA, FICA and RICA will help guide CC implementation (C1).

They also need to know what level of data confidentiality; security and privacy are available in that jurisdiction as this will all affect their CC adoption success. SLAs should be standardised and it should clearly define what remedies or solution will be provided in case of a breach from the service provider. This will ensure that the service provider delivers agreed level of service at all times. It is also important to investigate whether competitors are already using CC and whether it is giving them some form of competitive advantage over the organisation. This will give the organisation a clear picture of where their CC implementation will place the in relation to competitors. Finally, if the organisation decided to implement public cloud, they should ensure that their data will be properly backed up and their access will be guaranteed by the service provider in case there is a problem of reputation fate sharing.

5.4 Summary of chapter

The BCCR framework was developed based on the outcomes of the literature review and interview using the TOE framework and the methods for managing change by Kotter & Schlesinger, (2008). The authors suggest that the BCCR framework will assist financial institutions to determine whether or not they are ready for CC adoption. The BCCR framework will also assist financial institutions to improve their readiness level. It will also assist them to manage all the changes as a result of CC effectively. Overall, the BCCR will increase the chances of success of CC adoption and help financial institutions reap the benefits of CC.

6. Conclusions and recommendations

This chapter presents the findings of this research and attempts to answer the research questions. Recommendations based on the findings are also presented in this chapter by drawing together the results from the previous chapters. The Implications for the research, gaps, anomalies and/or deviations in the data and research Contributions are also discussed in this chapter. The last section of this chapter discusses areas of future research.

6.1 Findings

The findings from this study confirmed that CC readiness level of SA financial institutions is low. This research also found that adoption of CC in SA is generally low. SA is about 7 years behind countries like USA and UK in terms of CC adoption (C1).

It was also confirmed that security and privacy are among the biggest concerns about CC among SA financial institutions. This was evident as the financial institutions that are already using some CC offerings are only using it for their non-core and less sensitive business activities such as customer management and human resources management. The more sensitive and core data are still kept in the traditional systems in-house.

Although CC adoption is low, most financial institutions are in the process of considering its use for their core business activities. This is because they believe that CC has the capabilities to turn their businesses around and improve their quality of service.

This research found that communication skills are essential in managing CC teams and service providers. This confirms several literatures that found that communication can help increase the chances of CC implementation success. In line with other literatures, this research also found that good knowledge of internet is essential for CC implementation success. This is because CC is hosted on the internet and the quality of internet service impacts the quality of CC services.

Another interesting finding of this research is that financial institutions in SA uses CC for collaboration among branches as they all have several branches across the country. This assists them in making quick and efficient decision. The most common CC services used by SA financial institutions are CRM from salesforece.com and human resources management. This confirms the findings of Sharma (2012) who also found that many financial institutions use CC for their CRM. Email system

from microsoft 365 and amazon web services where clients just buy non-core infrastructure are also commonly used by SA financial institutions (C1).

The most common type of CC used by SA financial institutions is SaaS and the usage of CC is increasing among SA financial institutions. The usage of IaaS among SA financial institutions is low while PaaS has the lowest usage when compared with SaaS and IaaS (C1, C2, C3 & C4).

The data analysis revealed that organisations are paying little attention to training in terms of CC because most of the participating organisations do not have CC training programmes in place. The data analysis also revealed that cost and security are the most important factors to organisations when considering CC adoption. There is no specific legislation or law in SA to regulate CC, the POPI which was signed into law in November 2013 will contribute towards regulating some aspects of CC. This research also found that government support is not available in SA in terms of making necessary infrastructure such as bandwidth available for organisations wishing to adopt CC. Although there are laws such as POPI, ECA, RICA and FICA which will help regulate some of the activities with CC, there are no laws specific to CC in SA.

One of the surprising findings of this research is that some of the financial institutions in SA are outsourcing the CC infrastructure management to third party service providers. It is also surprising to find out that SA financial institutions have no CC risk governance in place and they outsource their CC risk governance to third party service providers. It is also surprising to find out that evaluation of CC cost and benefits are also outsourced. Furthermore, the researcher found it surprising that skills assessment and training on CC are also outsourced.

It is also surprising that the service providers are given the sole mandate of managing data loss and breach of privacy. One would expect that the financial institutions should do that in-house as data loss could have a damaging effect on their organisation.

This research also confirmed findings of other researchers that the quality of internet service in SA is not so good because of the poor bandwidth availability. Fast reliable data such as fibre is expensive while Asymmetric digital subscriber line (ADSL) can be slow and unreliable. Successful implementation of CC is dependent on fast, reliable bandwidth. The lack of adequate bandwidth can affect the quality internet service which will also affect the quality of CC service.

This research also found that in order to select a service provider, organisations need to check the track record of service providers in the market. The number of clients of the service provider in their industry or other industries as well as the service provider's ability to provide evidence of controls and procedures should also be considered. Furthermore, transparency shown during due diligence, recommendations by research organisations and access to audit reports conducted by a third party should also be considered when choosing a service provider.

Because SA financial institutions are still in their early stages of CC adoption, most of them are currently re-architecting their existing architecture to integrate it with CC. Financial institutions in SA prefer private clouds because it offers more security and control than public clouds. The ability of users to have more control of their data and information in private clouds makes it a preferred choice for SA financial institutions. Another reason why SA financial institutions prefer private clouds is that the skills needed for private clouds are similar to the traditional IT skills i.e. they need to set up a data centre and manage it in-house.

This research also found that service provider management is important because of the huge responsibility placed on service provider by SA financial institutions in managing important aspects of CC such as data loss and disaster recovery. This therefore makes it important for financial institution to develop appropriate strategies for managing service providers so as to ensure that they deliver agreed level of service.

To answer the research questions, the CC readiness of SA financial institutions is still in its early stages as most of the financial institutions are not yet ready for CC adoption. Some of the barriers of CC adoption include security and privacy, governance issues, inadequate cloud SLAs, vendor lock in, poor vendor transparency, inability to assess risks, confidentiality, integrity and availability issues, integration issues etc.

The enablers of CC adoption include scalability and flexibility, broad network access, pay per use, economies of scale and cost effectiveness, reliability, increases speed of time to market, user centric interfaces, improved communication, improved focus on core business, scalability, cost reduction etc.

The BCCR framework that is capable of assisting financial institutions in determining and improving their CC readiness level was developed and this shows that it is possible to develop such a framework.

6.2 Recommendations

The BCCR framework which was developed in this research was developed using TOE framework, change management model and the response from interview participants. The researcher believes that if financial institutions utilise this framework and use it as a guide to determine and improve their level of CC readiness, it will improve their chances of successfully implementing CC.

Once an organisation has attained sufficient CC readiness level, it is important to make the right choice of cloud provider as it may not be easy to move across platforms of different provider due to integration issues. It is recommended that organizations should try and achieve a high level of CC readiness before adopting CC to improve their chances of success. Organisations are also advised to begin their adoption in stages i.e. they should start by moving their non-core applications to the cloud and experiment with those before moving their core applications (Vignos, Kim, & Metzer, 2013).

6.3 Outcome of the research in relation to literature

The outcome of this research is consistent with literature. Most of the issues with CC such as security and privacy issue, vendor lock in, lack of standard SLAs etc. that have been identified in literature were also mentioned by the participants during the interviews. This shows that the outcome of this research is consistent with literature. Another interesting thing that came up during this research was the identification of skills that are needed for a CC implementation to be successful. PI2 mentioned skills such as project management skills, change management skills and negotiation and financial skills which are necessary for CC implementation. This is also in line with literature as previous research had identified them. It is very easy for one to ignore or forget about these skills and think of the more technical skills such as integration skills, security and compliance and mobile applications development. Forgetting about them may however pose a problem which could affect implementation success because those skills are as important as the technical skills in order to ensure that CC implementation goes as planned and the benefits of CC are realised.

6.4 Limitations

The possible gap in the data is that there could be changes in the data obtained within a short period of time. This is because almost all of the participating organisations are in the early stages of their CC adoption and are progressing every day towards adoption. As a result, it is possible for the information gotten during the interview to have changed. For example, an organisation may not have CC strategy during March 2013 when the interview was conducted but may already put one in place one or two months later. Another limitation is that the scope of this study is limited to financial institutions and the results may not be applicable to other industries.

6.5 Research contributions

The results of this research has shown that adoption of CC among financial institutions in SA is slow because of issues such as security, reliance on internet, lack of standard SLA's, lack of government support, lack of laws and regulations specific to CC. This helps to validate the literature.

This research has contributed to knowledge by developing a framework (BCCR) which will assist financial institutions to improve their CC readiness level and increase the chances of adopting CC successfully. The output of this research will also contribute to research by challenging researchers to conduct similar research in other industries with the hope of coming up with a framework or model that will be applicable in different organisations across several industries.

This research is one of the few researches that have attempted to integrate change management framework with TOE framework to develop a framework that will not only manage the process of CC readiness but will also ensure that the changes that the organisation will faces as a result of CC will be properly managed in order to prevent possible CC implementation failure as a result of poor change management.

6.6 Future research

There is a wide range of research area on CC because it is still in its early stages. In future, researchers could apply BCCR framework on organisations that are planning to adopt CC and observe and document any improvements in their CC readiness level. Since this research focused specifically of financial institutions, future research could focus on another industry or organisation as the result of this research cannot be generalised. The results from different research across several industries could be combined in future in order to come up with solution that could be applied across several industries.

6.7 Summary of chapter

This dissertation has been able to determine that the readiness level of financial institutions in SA is low because most of the organisations involved in this study are still in their early stages of CC implementation. This dissertation was also able to identify the barriers and enablers of CC. Finally this thesis was able to develop a framework which will serve as a tool by which financial institutions can determine and improved their CC readiness level. This will increase the confidence of financial institutions on their ability to successfully adopt and use CC to their advantage.

7. References

Agopyan, A., Sener, E., & Beklen, A. (2010). Financial Business Cloud for High-Frequency Trading. *The First International Conference on Cloud Computing, GRIDs, and Virtualization* (pp. 164 - 169). Istanbul: IARIA.

Ahmed, M., Chowdhury, A. M., Ahmed, M., & Rafee, M. H. (2010). An Advanced Survey on Cloud Computing and State-of-the-art Research Issues. *International Journal of Computer Science Issues*, 9 (1), 201 - 207.

Al-Somali, S. A., Gholami, R., & Clegg, B. (2011). Determinants of B2B e-commerce adoption in Saudi Arabian firms. *International Journal of Digital Society*, 2 (2), 406 - 415.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., . . . Zaharia, M. (2009, February 10). Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. *Qualitative Research*, 1 (3), 385 - 405.

Benjamin, R. I., & Levinson, E. (1993). A framework for Managing IT-Enabled Change. *Sloan Management Review*, 33 (4): 23 - 33.

Braun, V., & Clarke, V. (2006). Using thematic analysis in Psychology. *Qualitative Research in Psychology*, 3 (2), 77 - 101.

Bryman, A., & Bell, E. (2007). *Business Research Methods.* New York, USA: Oxford University Press.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2008). Cloud computing and emerging IT platforms: Vision, hype, and reality fordelivering computing as the 5th utility. *Future Generation Computer Systems*, 1 - 18.

Canedo, E. D., de Sousa Junior, R. T., & de Oliveira, R. (2012). Trust model for reliable file exchange in Cloud Computing. *International Journal of Computer Science & Information Technology (IJCSIT)*, 4 (1), 1 - 18.

Carroll, M., Van der Merwe, A., & Kotze, P. (2011). Secure cloud computing: Benefits, risks and controls. *Information Security South Africa (ISSA)* (pp. 1 - 9). Johannesburg: Institute of Electrical and Electronics Engineers.

Chauhan, V. K., Bansal, K., & Alappanavar, P. (2012). Exposing cloud computing as a failure. *International Journal of Engineering Science and Technology*, 4 (4), 1320 - 1326.

Chisnall, P. (1997). *Marketing Research (5th Ed).* London: McGraw Hill.

Dillon, T., Wu, C., & Chang, E. (2010). Cloud Computing: Issues and Challenges. *IEEE International Conference on Advanced Information Networking and Applications* (pp. 27 - 33). Perth: IEEE.

Dorey, P. G., & Leite, A. (2011). Commentary: Cloud computing - A security problem or solution? *Information Security Technical Report* , 16 (3), 89 - 96.

Fathian, M., Akhavan, P., & Hoorali, M. (2008). E-readiness assessment of non-profit ICT SMEs in a developing country: The case of Iran. *Technovation*, 28 (1), 578 - 590.

Ghanbari, H., Simmons, B., Litoiu, M., & Iszlai, G. (2012). Feedback-based optimization of a private cloud. *Future Generation Computer Systems*, 28 (1), 104 - 111.

Goel, M. S., Kiran, R., & Garg, D. (2011). Impact of Cloud Computing on ERP implementations in Higher Education. *International Journal of Advanced Computer Science and Applications*, 2 (6), 146 - 148 .

Goldstuck, A. (2011, November 16). *Corporate South Africa looks to the cloud for IT services*. Retrieved from IP EXPO 15th & 16th November, Sandton Convention Centre Ballroom: http://www.ipexpo.co.za/Highlights/Corporate-South-Africa-looks-to-the-cloud-for-IT-services

Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). The Characteristics of Cloud Computing. *2010 39th International Conference on Parallel Processing Workshops* (pp. 275 - 279). Las Vegas: IEEE Computer Society.

Goyal, P. (2010). Enterprise Usability of Cloud Computing Environments: ssues and Challenges. *2010 Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* (pp. 54 - 59). Las Vegas: IEEE Computer Society.

Grobler, M., & Dlamini, Z. (2010). Global Cyber Trends a South African Reality. *IST-Africa* (pp. 1 - 8). Pretoria: International Information Management Corporation.

Hay, B., Nance, K., & Bishop, M. (2011). Storm Clouds Rising: Security Challenges for IaaS Cloud Computing. *International Conference on System Sciences* (pp. 1 - 7). Hawaii: Institute of Electrical and Electronics Engineers.

Heinle, C., & Strebel, J. (2010). IaaS adoption determinants in enterprises. *Conference on the Economics of Grids, Clouds, Systems, and Services* (pp. 93 - 104). Ischia: Springer.

Hinde, C., & Van Belle, J.-P. (2012). Cloud Computing in South African SMMEs: Risks and Rewards for Playing at Altitude. *International Journal of Computer Science and Electrical Engineering*, 1 (1), 1 - 10.

Howell-Barber, H., Lawler, J., Desai, S., & Joseph, A. (2013). A Study of Cloud Computing Software-as-a-Service (SaaS) in Financial Firms. *Journal of Information Systems Applied Research*, 4 - 13.

HumanIPO. (2013, November 28). *Zuma signs POPI bill into law*. Retrieved from HumanIPO: http://www.humanipo.com/news/37362/zuma-signs-popi-bill-into-law/

Hussey, J., & Hussey, R. (2003). *Business Research: A Practical Guide for Undergraduate and Postgraduate Students.* Basingstoke: Palgrave Macmillan.

Islam, S., & Grégoire, J.-C. (2012). Giving users an edge: A flexible Cloud model and its application for multimedia. *Future Generation Computer Systems*, 28 (1), 823 - 832.

iTWeb. (2012, March 6). *iTWeb Cloud Computing*. Retrieved from iTWeb: http://www.itweb.co.za/index.php?option=com_content&view=article&id=52385

Joint, A., & Baker, E. (2011). Knowing the past to understand the present issues in the contracting for cloud based services. *Computer Law and Security Review*, 27 (1), 407 - 415.

Kafouris, D., & Houston, J. (2014, January 30). *POPI*. Retrieved from Delloitte: http://deloitteblog.co.za/tag/popi/

Khajeh-Hosseinil, A., Greenwood, D., & Sommerville, I. (2010). Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. *Third International Conference on Cloud Computing* (pp. 450 - 457). Miami: Institute of Electrical and Electronics Engineers.

Khorshed, T. M., Ali, S. A., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, 28 (1), 833 - 851.

Kotter, J. P., & Schlesinger, L. A. (2008). Choosing Strategies for Change. *Havard Business Review*, 86(7), 130 - 138.

Kshetri, N. (2010). Cloud Computing in Developing Economies: Drivers, effects and policy measures. *Pacific Telecommunications Council*, (pp. 1 - 22). Honolulu.

Lenk, A., Klems, M., Nimis, J., Tai, S., & Sandholm, T. (2009). What's inside the Cloud? An architectural map of the Cloud landscape. *Proceedings of the International Conference on Software (ICSE) Workshop on Software Engineering Challenges of Cloud Computing* (pp. 23 - 31). Vancouver, Canada: IEEE Computer Society .

Lin, A., & Chen, N. (2012). Cloud computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, 32 (6), 533 - 540.

Mahlong, A. (2012, 07 25). *Office 365 now available*. Retrieved from SA IT news: http://saitnews.co.za/cloud-computing/office365/

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing - The business perspective. *Decision Support Systems*, 5 (1), 176 - 189.

Mason, J. (2002). *Qualitative Researching.* London: Sage Publications.

Maurer, M., Emeakaroha, V. C., Brandic, I., & Altmann, J. (2012). Cost–benefit analysis of an SLA mapping approach for defining standardized Cloud computing goods. *Future Generation Computer Systems*, 28 (1), 39 - 47.

McKendrick, J. (2013, December 3). *The 8 Most Important Skills Needed for Cloud Computing Today*. Retrieved from Forbes: http://www.forbes.com/sites/joemckendrick/2012/08/27/the-8-most-important-skills-needed-for-cloud-computing-today/

Misra, S. C., & Mondal, A. (2011). Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment. *Mathematical and Computer Modelling*, 53 (1), 504 - 521.

Myers, D. M. (2009). *Qualitative Research in Business & Management.* London: Sage Publications.

Nasir, U., & Niazi, M. (2011). Cloud Computing Adoption Assessment Model (CAAM). *Profes* (pp. 34 - 37). Torre Canne (BR), Italy: ACM.

Oates, J. B. (2006). *Researching Information Systems and Computing.* London: Sage Publications.

Pudjianto , B., Zo, H., Ciganek, A. P., & Rho, J. J. (2011). Determinants of E-Government Assimilation in Indonesia: An Empirical Investigation Using a TOE Framework. *Asia Pacific Journal of Information Systems*, 21 (1), 50 - 80.

Rani, S., & Gangal, A. (2012). Security issues of banking adopting the application of cloud computing. *International Journal of Information Technology and Knowledge Management*, 5 (2), 243 - 246.

Roberts II, J. C., & Al-Hamdani, W. (2011). Who can you trust in the cloud?: a review of security issues within cloud computing. *Information Security Curriculum Development Conference* (pp. 15 - 19). New York: Association for Computing Machinery.

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students.* London, UK: Prentice Hall.

Sharma, A. (2012). Data Management and Deployment of Cloud Applications in Financial Institutions and its Adoption Challenges. *International Journal of Scientific & Technology Research*, 1 (1), 1 - 7.

Snyder, H. R. (2001). Indicators of organizational readiness for clinical information technology/systems innovation: a Delphi study. *International Journal of Medical Informatics.*, 63 (3), 179 - 204.

Speckman , A. (2012, 04 25). *Sky is limit for cloud computing* . Retrieved from iol: http://www.iol.co.za/business/business-news/sky-is-limit-for-cloud-computing-gijima-1.1283179?ot=inmsa.ArticlePrintPageLayout.ot

Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. *Information Security Technical Report*, 16 (3), 102 - 107.

Tian, L.-Q., Lin, C., Ni, Y., & Duxiujuan. (2011). A kind of user behavior authentication model and analysis in cloud computing. *Energy Procedia*, 13 (1), 4099 - 4107.

Todnem By, R. (2005). Organisational Change Management: A Critical Review. *Journal of Change Management*, 5 (4), 369 - 380.

Tornatzky, L. G., Mitchell, F., & Chakrabarti, A. K. (1990). *The processes of technological innovation.* Massachusetts: Lexington Books.

Tsai, W.-T., Sun, X., & Balasooriya, J. (2010). Service-Oriented Cloud Computing Architecture. *Seventh International Conference on Information Technology* (pp. 684-689). Arizona: IEEE Computer Society.

Vaidya, K., Sajeev, A. S., & Gao, J. (2005). e-Procurement Assimilation: An Assessment of -business Capabilities and Supplier Readiness in the Australian Public Sector. *ICEC* (pp. 429 - 434). Xi'an, China: ACM.

Vignos, J., Kim, P., & Metzer, R. L. (2013). Demystifying the Fog: Cloud Computing from a Risk Management Perspective. *Journal of Information Systems Applied Research*, 6 (3), 26 - 33.

Viljoen, M., Solms, R. V., & Lawack-Davids, V. (2012). Regulatory Compliance in Cloud Computing: An IT perspective. *Southern Africa Telecommunication Networks and Applications Conference* (pp. 48 - 54). George, South Africa: EE Publishers.

Vorster, G. (2012, 02 26). *SA ranked low for cloud readiness*. Retrieved from BusinessTech: http://businesstech.co.za/news/cloud-hosting/6654/sa-ranked-low-for-cloud-readiness/

Wang, L., Von Laszewski, G., Kunze, M., & Tao, J. (2010). Cloud Computing: a Perspective Study. *New Generation Computing*, 28 (2), 137 - 146.

Wang, W. Y., Rashid, A., & Chuang, H.-M. (2011). Toward the Trend of Cloud Computing. *Journal of Electronic Commerce Research*, 12 (4), 238 - 242.

Weiner, B. J. (2009). A theory of organizational readiness for change. *Implementation Science*, 4 (67), 1 - 9.

Yeo, C. S., Venugopal, S., Chu, X., & Buyya, R. (2010). Autonomic metered pricing for a utility computing service. *Future Generation Computer Systems*, 26 (1), 1368 - 1380.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1 (1), 7 - 18.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28 (1), 583 - 592.

8. Appendices

8.1 Appendix A: Ethics form

UNIVERSITY OF CAPE TOWN
FACULTY OF COMMERCE
Igniting Knowledge and Opportunity

Commerce Faculty Ethics in Research Committee

Any individual in the Faculty of Commerce at the University of Cape Town undertaking any research that involves the participation of human subjects is required to complete this form. The completed form should be submitted to departmental Ethics Committee representatives for submission to the Commerce Faculty Ethics in Research Committee

2013 Application

1. PROJECT DETAILS		
Project title:	Assessment of Cloud Computing Readiness of Financial Institutions in South Africa.	
Principal Researcher/s:	Akande Akinlolu Olumide	**Research Supervisor / Co-researchers:**
E-Mail Address:	Akinlolu.Akande @uct.ac.za	Professor Jean-Paul Van Belle
Brief description of the project: The project aims to assess the cloud computing readiness of financial institutions in South Africa and to develop an integrated framework which will serve as an instrument by financial institutions can measure their cloud computing readiness.		
Research methods and procedure: (please tick and explain procedure) ☒Interviews ☐Survey questionnaire ☐Experiment ☐Secondary data ☐Observation ☐ Other (please specify):		

2. PARTICIPANTS

Characteristics of participants:

Gender: Any	Any
Race / Ethnicity:	Any
Age range:	20 years and above
Location:	South Africa
Other:	IT staffs involved with their organisations cloud computing implementation.

Affiliations of participants: (please tick)

☒Company employees ☐ Hospital employees ☐ General public ☐ Military staff ☐ Farm workers ☐ Students

☐ Other (specify)

If your sample includes children (aged 15 and below), mentally incompetent persons, or legally restricted groups please explain on a separate page why it is necessary to use these particular groups

*If there is a question on Race/Ethnicity in a questionnaire, an option "**Prefer not to Answer**" must be included*

3. ORGANISATIONAL PERMISSION

If your research is being conducted within a specific organisation, please state how organisational permission will be obtained:

A letter will be sent to management of all the participating organisations to request their permission to conduct interviews with their employees.

If your participants are UCT students and/or staff, access permission must be sought as follows:
For Staff permission – Executive Director: Human Resources (Miriam.Hoosain@uct.ac.za)
For Student permission – Executive Director: Student Affairs (Moonira.Khan@uct.ac.za)

4. INFORMED CONSENT

What type of consent will be obtained from study participants?

- (•) Oral Consent
- ( ) Written Consent
- ( ) Anonymous survey questionnaire (covering letter required, no consent form needed)
- ( ) Other (please specify)

How and where will consent/permission be recorded?

Permissions will be recorded in a consent form which will be given to all the participants at the premises of the participating organisation

If subjects are minors or mentally incompetent, describe on a separate page how and by whom permission will be granted?

5. CONFIDENTIALITY OF DATA

What precautions will be taken to safeguard identifiable records of individuals? Please describe specific procedures to be used to provide confidentiality of data by you and others, in both the short and long run. This question also applies if you are using secondary sources of data.

In order to safeguard identifiable records of individuals, personal information like name, address, phone number etc. of participants will not be requested in the interview. Any personal information about the participants and their organisations will also not be included in the final paper.

6. RISK TO PARTICIPANTS

Does the proposed research pose any physical, psychological, social, legal, economic, or other risks to study participants you can foresee, both immediate and long range? (tick one)

☐ **Yes** ☒ **No**

If yes, answer the following questions on a separate page:

1. Describe in detail the nature and extent of the risk and provide the rationale for the necessity of such risks
2. Outline any alternative approaches that were or will be considered and why alternatives may not be feasible in the study
3. Outline whether and why you feel that the value of information to be gained outweighs the risks

7. intended dissemination of research findings

Have you discussed authorship issues with your co-researchers or supervisor? (tick one)

☐ Research not intended for publication (please provide details below)

☒ Standard authorship agreement: Joint authorship – If based on a student research project, student will be first-named author unless student has little involvement in preparation of paper for publication, in which case supervisor will be first-named author

☐ Bespoke authorship agreement (please provide details below)

Details about authorship

☒ **Standard**

I certify that we have read the the UCT Authorship Policy, and Commerce Faculty Authorship Guidelines (http://www.commerce.uct.ac.za/Commerce/Information/research.asp**):**

Signed by candidate

Applicant's signature: Signature Removed **Date: 15/03/2013**

PLEASE ATTACH THE FOLLOWING DOCUMENTS TO YOUR APPLICATION

1. **A full copy of the research proposal**
2. **Any consent form that will be signed by the participants or read to them (if any)**
3. **Any interview schedules, cover letters, forms, instruction sheets, survey questionnaires or other material that will be used in the study.**

I certify that that the material contained herein is truthful and that all co-researchers and supervisors are aware of the contents thereof.

Signed by candidate

Applicant's signature: Signature Removed Date: 15/03/2013

FOR ETHICS COMMITTEE REPRESENTATIVE ONLY
Recommendation: **Signature:** **Date:**
FOR ETHICS COMMITTEE CHAIRPERSON ONLY
Recommendation: **Signature:** **Date:**

8.2 Appendix B: Cover letter

Cover Letter for Participation in Interview

Department of Information Systems

Leslie Commerce Building

Engineering Mall, Upper Campus

OR Private Bag, Rondebosch, 7701

Cape Town

Tel: 650-2261

Fax No: (021) 650-2280

REQUEST TO PARTICIPATE IN A RESEARCH INTERVIEW

Dear Participant,

I am currently pursuing my Master's degree in Information Systems at the University of Cape Town. I am conducting a research on cloud computing readiness of financial institutions in South Africa. Cloud computing is a new technology that is still in its infancy and promises a lot of benefits such as cost reduction, faster time to market and flexibility to mention just a few. This interview will contribute towards identifying the barriers and enablers of cloud computing readiness and lead to the development of an integrated framework which will serve as an instrument by financial institutions can measure their cloud computing readiness. The study will benefit your organisation by providing a framework which will provide structure to your cloud computing initiatives and increase your organisations cloud computing readiness level. The study will collect information through face to face interviews.

I would like to use this medium to request your participation in the interview. The interview will take 40 to 60 minutes to finish depending on the participants level of understanding of cloud computing. The data gathered from the interview will be kept confidential and the participant's identity as well as their organisations identity will be made anonymous because personal details such as name, address or telephone contact of the participants will not be included in the research publication.

Please note that your involvement in the interview is voluntary. The interview questions have been approved by UCT's Commerce Faculty Ethics in Research Committee. A copy of the final report will be sent to you on your request. I thank in anticipation of your participation in the interview.

Kind Regards,

Akande Akinlolu Olumide.

For enquiries, please contact:

Researcher: Akande Akinlolu Olumide

E-mail: Akinlolu.Akande@uct.ac.za

Cell: +27 723135908

OR

Supervisor: Professor Jean-Paul Van Belle

Department of Information Systems

University of Cape Town

E-Mail: Jean-Paul.VanBelle@uct.ac.za

Phone: +27 (0)21 650 4256

8.3 Appendix C: Informed consent form

INFORMED CONSENT FORM

I/we ……certify that my/our participation in the study of assessment of cloud computing readiness of financial institutions in South Africa by Mr Akande Akinlolu is voluntary. I/we also certify that I/we am/are in the right state of mind to participate in this research.

By signing this form you confirm your participation in the research on "Assessment of cloud computing readiness of financial institutions in South Africa" either through face to face interviews or telephone interviews.

Signature..... Date: .....

8.4 Appendix D: Interview guide

The interview guide

Introduction

- Introduction and greetings
- Purpose of the interview
- The participants will be briefed about the ethical procedures regarding the information from the interview.
- The participants will be assured of confidentiality data given during the interview.

Rights of the participants

- The participants will be provided with the following information
- The participants may respond to any question
- The participants have the right to decline voice recording
- The participants may offer any information after the interview.
- The participants may ask for a copy of the research results
- The participants will be sent the summaries or recordings of the interview for validation

Section A: General questions

1. Name of organisation _____
2. Organisational sector _____
3. What is your organisation's core business? _____
4. How many employees does your organisation have? _____

5. How long have you been working for your organisation? _____

6. What is your role in your organisation's IT decision? _____

7. Do you have any cloud computing experience? _____

Section B:

This section aims assess the cloud computing readiness level of financial institutions from three perspectives which are technology, organisation, and environment. The answers to the questions in this section will be used in answering the research questions and developing an integrated framework which will serve as an instrument by financial institutions can measure their cloud computing readiness.

8. What is your understanding of cloud computing?

9. What skills do you require in order to use cloud computing?

10. What cloud computing services do you use?

11. What features influence you to use cloud computing?

12. What factors do you consider to be the most important when using cloud computing?

13. How do you feel about the cost of cloud computing services?

14. What are your views of cloud computing usage in your organisation?

15. What is cloud computing regulatory environment?

16. In your opinion, what are the advantages of cloud computing?

17. In your view, what are the disadvantages of cloud computing?

18. Is your organisation already using cloud computing?

19. What type of cloud environment does your organisation currently have or is planning to have?

20. Do have anything else you would like to say?

21. What is the state of your cloud computing architecture?

22. How would you describe your IT architectural capabilities for cloud computing?
23. Are you re-architecting your applications for cloud computing?
24. How would you describe management capabilities of your cloud environment?
25. What security measures do you have for your cloud computing environment?
26. Do you have business continuity and disaster recovery (BCDR) plans in place for cloud environment?
27. Who is responsible in the case of data loss or breach of privacy?
28. Does your organisation have a cloud computing strategy in place?
29. Have your organisation evaluated the costs and benefits of cloud computing?
30. Does your organisation have employees with cloud computing experience?
31. Does your organisation have training programmes for employees on cloud computing?
32. Has your organisation defined or measured the business value of cloud computing?
33. What is your organisations process for ensuring security and compliance for cloud computing?
34. What is the mechanism for adding users who need to access cloud based services?
35. How would you describe your organisations cloud computing governance?
36. What steps have been taking around communicating the results of your cloud computing initiative?
37. How will you identify the right cloud computing vendor for your organisation?
38. What are indicators that a cloud computing vendor is trustworthy?
39. Do you know the legislations and laws relating to cloud computing?
40. Is there any government support for cloud computing that can benefit your organisation?

Conclusion

A brief review of the interview is discussed

Appreciation

Appreciate and thank the participants

8.5 Appendix E: PaaS, IaaS and SaaS provider as well as services provided

Organization	Service or tool	Description
Akamai	EdgePlatform	Content, Site, Application Delivery
Facebook	Facebook Platform	Development tools and execution environment for social networking applications
Google	App Engine	Scalable runtime environment for Python Web applications
Microsoft	Azure	Development environment and runtime for Microsoft applications
	Live Mesh	Platform to sync, share and access a wide range of devices with Microsoft operating systems
NetSuite	SuiteFlex	Toolkit to customize NetSuite online business applications
Salesforce	Force.com	Build and deliver on-demand business applications
Sun	Caroline	Horizontally scalable platform for the development and deployment of Internet services.
Zoho	Zoho Creator	Toolkit to build and deliver on demand business applications

Table 7: Platform-as-a-Service providers adopted from Lenk, Klems, Nimis, Tai, & Sandholm, (2009 pg. 31).

Organization	Service or tool	Description
Amazon	Elastic Compute Cloud (EC2)	Virtual servers
	Dynamo	Key-value storage system
	Simple Storage Service (S3)	Storage buckets
	SimpleDB	Database-as-a-Service
	CloudFront	Content Delivery
	SQS	Queueing services
AppNexus	AppNexus Cloud	Virtual servers
Bluelock	Bluelock Virtual Cloud Computing	Virtual servers
	Bluelock Virtual Recovery	Disaster Recovery
Emulab	Emulab Network Testbed	Network testbed
ENKI	ENKI Virtual Private Data Centers	On-demand virtual data center resources
EU Reservoir Project	Open Nebula	Open source virtual infrastructure engine
FlexiScale	FlexiScale Cloud Computing	Virtual servers
GoGrid	Cloud Hosting	Virtual servers
	Cloud Storage	Disk storage
Google	Google Big Table	Distributed storage system
	Google File System	Distributed file system
HP	iLO	Lights out management
	Tycoon	Market-based system for managing compute resources in clusters
	Accelerator	Virtual servers
Joyent	Connector	Pre-configured virtual

		servers
	BingoDisk	Disk storage
Nirvanix	Nirvanix Storage Delivery Network	Disk storage
OpenFlow	OpenFlow	Network simulation
Rackspace	Mosso Cloud Sites	Pre-configured virtual servers
	Mosso Cloud Storage	Disk storage
	Mosso Cloud Servers	Virtual servers
Skytap	Skytap Virtual Lab	Virtual IT lab environment
Terremark	Infinistructure	Virtual servers
The Globus Alliance	Nimbus	Open source toolkit to turn a cluster into an IaaS cloud.
UCSB	EUCALYPTUS	Open source implementation of Amazons EC2
10gen	Mongo DB	Database for cloud storage
	Babble Application Server	Web application server for cloud deployments

Table 8: Infrastructure-as-a-Service providers adopted from Lenk, Klems, Nimis, Tai, & Sandholm, (2009 pg. 30).

Organization	Service or tool	Description
Google	Google Docs	Online office suite
	Google Maps API	The Google Maps API lets developers embed Google Maps in their own web pages with JavaScript.
	OpenSocial	A common API for social applications across multiple websites.
OpenID Foundation	OpenID	Distributed system to allow users to have a single digital identity across the Internet.
Microsoft	Office Live	Online office suite
Salesforce	Salesforce.com	Customer Relationship Management

Table 9: Software-as-a-Service providers adopted from Lenk, Klems, Nimis, Tai, & Sandholm, (2009 pg. 30).